Common Criteria for Information Technology Security Evaluation

Protection Profile for Switches and Routers

Draft Version 2.1
February 22, 2001

Prepared By: Booz·Allen & Hamilton, Inc.
900 Elkridge Landing Road.
Linthicum, MD 21090

Prepared For: National Security Agency (NSA)

FOREWORD

This Protection Profile for switches (e.g., ATM switches and Optical switches) and routers was generated under the Information Assurance Solutions program, sponsored by the National Security Agency (NSA) and prepared by Booz·Allen & Hamilton, National Security Team to promulgate security standards for switches and routers.

Please send comments on this Protection Profile to
Renee Esposito, esposito_renee@bah.com, or
Gary Buda, buda_gary@bah.com, at
Booz·Allen & Hamilton
900 Elkridge Landing Road
Linthicum, MD 21090.

This Protection Profile is the first formal submission by Booz·Allen & Hamilton to the NSA on this particular concept of security standards for switches and routers. Acknowledgements are given to Kim Hebda, Neil Ziring, Jill Hanchey, Melissa Crouch, Tim Lusby, Chris Kubic and Keith Fuller of the NSA.

The base set of requirements used in this protection profile are taken from the "Common Criteria for Information Technology Security Evaluation, Version 2.1."

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CONVENTIONS AND TERMINOLOGY

Conventions

The notation, formatting, and conventions used in this Protection Profile (PP) are based on or consistent with version 2.1 of the Common Criteria (CC). Font style and conventions to help clarify the information were developed to aid the reader. Additionally, British English, as used in the Common Criteria, has not been used in this Protection Profile.

The Common Criteria allows for iterations, selections, assignments, and refinements to be performed on functional requirements. These operations are defined in Common Criteria, Part 2, paragraph 2.1.4.

Iteration "allows a component to be used more than once with varying operations." Iterations are indicated with a space between each line within the requirement, refer to FMT_MSA.1 within this protection profile.

A selection "allows the specification of one or more elements from a list." Selections are expressed in this Protection Profile by using *underlined italics.*

An assignment "allows the specification of an identified parameter." Assignments are expressed by using underlining. When an assignment can be further defined by the developer in subsequent security target documentation brackets are used. When an assignment has been left to the discretion of the developer, "[ST assignment]" will be the term stated as such.

A refinement allows the addition of details. Refinements are stated as such immediately following the requirement.

Application notes are provided, also directly following the requirement, to support information that is considered relevant or useful for the construction, evaluation, or use of the TOE, and to clarify the intent of the requirement as related to this Protection Profile.

TERMINOLOGY

Client is the source responsible for originating or receiving data transmissions. A client is the source sending data transmissions via a switch or router.

Network Performance Management Operator is a network management role that only has viewing privileges including the authorization to gather and analyze network performance statistics.

Network Management Administrator is a network management role that may include many subsets of roles and privileges within the network management system. A Network Management Administrator is able to perform the duties of a Network Performance Management Operator and is also able to configure, provision and trouble shoot the network among any other necessary privileged operations.

Network Management Security Administrator is a network management role that includes the role of the Network Performance Management Operator, and the Network Management Administrator persons. In addition, a Network Management Security Administrator has the privilege to perform other actions including, but not limited to, creating and modifying access control lists, loading keys, and restricting applications. A Network Management Security Administrator is also responsible for maintaining a role for the review of network management audit logs and a role for the acceptance of the Target of Evaluation (TOE) installation and continual maintenance of the TOE for the assurance of proper functioning.

A Trusted Path is a communication path for which exchanges may be initiated by either side of the path and both ends of the path are identifiable. A trusted path contains identified subsets of TOE Security Function (TSF) data and commands. For the purpose of this protection profile a trusted path is the network management link, referred to as a management path, through which network information is passed. Therefore, one end of the path is the network management station and the other end is the switch or router that is being managed.

A Trusted Channel provides a means for clients to perform functions through an assured connection from TOE to TOE. A trusted channel is used to transmit control information for messages and is also desired for client actions such as identification and authentication. A trusted channel will be referred to as a control channel and is either a routing channel, a signaling channel, or a remote user connection (e.g. telnet, Rlogin, etc.). (Note for expansion but not necessarily this PP: an ideal trusted channel would also guarantee protection from modification by or disclosure to untrusted parties).

A Trusted Source is a source/node that can be identified and authenticated. The integrity of information from a trusted source is able to be verified and ensured.

DOCUMENT ORGANIZATION

Section 1 provides the introductory material for the protection profile

Section 2 provides the TOE description and presents three architectural scenarios in which the TOE may be operating.

Section 3 provides a discussion of the expected TOE Security Environment. This section also defines the set of assumptions, threats and policies that are to be addressed by either technical countermeasures implemented in the TOE hardware or software or through environmental controls.

Section 4 defines Security Objectives for the TOE and the TOE environment, which are based on a consideration of the defined assumptions, threats, and policies.

Section 5 provides Information Technology (IT) Security Requirements, which contains the Functional and Assurance requirements derived from the CC, Part 2 and 3, respectively, that must be satisfied by the TOE.

Section 6 provides a Rationale to explicitly demonstrate how the identified security objectives address the identified policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and demonstrates that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Section 6 continues with assurance level rationale, a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements.

Appendix A provides an acronym list to define frequently used acronyms.

Appendix B provides an index of terms to define terms used within this Protection Profile.

1.0 INTRODUCTION

Title: Protection Profile for Switches and Routers

Authors: Renee Esposito, Gary Buda

Vetting Status: TBD

CC Version: This Protection Profile was developed using Version 2.1 of the Common Criteria

General Status: Draft – Version 2.1

Registration: TBD

This PP was generated under the Information Assurance Solutions program, sponsored by the NSA and prepared by Booz·Allen & Hamilton, National Security Team to promulgate security standards for switches (e.g., ATM switches, Optical switches) and routers. This PP may be of use to several audiences, Information System Security Engineers (ISSEs), product vendors, security product evaluators, and system integrators. For product vendors and evaluators, this PP defines a minimal set of security requirements for switches and routers that must be addressed by provided products as documented in vendor Security Targets (STs) and as evaluated. System integrators and ISSEs may find this protection profile useful for identifying areas that need to be addressed by currently available product lines to provide a more comprehensive security solution. By matching the PP with available ST's, security gaps may be identified and products selected to bridge these gaps.

1.1 PROTECTION PROFILE OVERVIEW

This PP specifies requirements for protecting information with switches and routers that are compliant with this PP. Information that requires protection is any information that is deemed important to an organization, the loss of which might cause financial difficulties, cause scheduled impacts or affect the well being of the employees. In conjunction with switches and routers that are compliant with this PP, additional security mechanisms may be used at the discretion of an organization to enhance the assurance of their information protection policy. Additional security mechanisms include but are not limited to firewalls, guards, and encryptor devices. This PP is intended for all audiences, public and private industry. As well, this PP also applies to every possible scenario, which are summarized with the following three management scenarios under which the switches or routers may be operated.

1) The purchaser owns and manages its own equipment, which communicates across a private network.
2) The purchaser owns equipment but a network provider or commercial organization manages it. The equipment is located at the network provider's or commercial organization's site.
3) The purchaser does not own or manage any equipment but purchases services from a provider.

These scenarios are described in more depth in section 2.2, including example diagrams. Switches and routers are dependent upon a network management system for proper operating functionality. A network management system is the system in which connection parameters are defined. While the network management system is an integral part to the operation of switches and routers it is not considered part of the TOE in this PP.

In any environment, the requirements specified herein for switches and routers are appropriate for the protection of day-to-day private and sensitive information pertaining to the management and control of a network infrastructure. This PP specifically excludes protection of user data traversing the network infrastructure. The assumptions, threats, and organizational policies that are to be addressed by switches and routers are defined in this PP. The implementation of independent security objectives of the switches and routers and the environment are defined. Functional security and assurance requirements are also defined. Finally, this Protection Profile provides the rationale for the proposed security objectives and specified security requirements. The rationale in section 6.5 is provided for this protection profile to meet the strength of an Evaluation Assurance Level 3 (EAL3) - Augmented.

1.2 RELATED PROTECTION PROFILES

This PP was written to be compatible with the Virtual Private Network Protection Profile for Protecting Sensitive Information and the Telecommunications Switch Protection Profile.

2.0 TOE DESCRIPTION

This section provides background information, three network architecture scenarios, the TOE description and desired security capabilities for switches and routers.

2.1 TOE FUNCTIONALITY

Asynchronous Transfer Mode (ATM) is a connection-oriented means of transferring information that is organized into fixed-length (53 byte) cells. Connection-oriented means that virtual connections between the endpoints must be established prior to any transfer of information. Established connections allow for cells to be transmitted with controlled-delay. The flow of traffic can be controlled so that it either falls within a fixed priority scheme or is transmitted as best effort traffic.

Internet Protocol (IP) Routing is a connectionless means of transferring information contained within variable length packets. The delivery of traffic between the host and destination is generally best effort traffic and delivery is not guaranteed. Since prior logical paths are not established each IP packet can be dynamically routed across multiple different paths. A router dynamically determines the best path based on assigned routing protocols and the status of the network.

Optical switches provide the capability of ATM and IP to directly access the optical network, bypassing SONET/SDH. Optical switches serve as multiservice, multiwavelength platforms as they are able to act as service aggregators, and switch network traffic while presenting the streams into the optical core.

There are at least two methods for the classification of optical traffic. One method is to send traffic in completely different communications channels. The bandwidth in the high-speed pipes across the optical core is structured to provide completely non-interacting channels. One channel is allocated to a high-priority traffic (e.g., voice applications), one to delay-sensitive data such as video, one to best-effort data, etc.

Another way to differentiate traffic based on classification is for all of the traffic types to share a common communications channel. This means that along the traffic path each network element that implements queuing has to perform some method of classification at a very fast rate. Typically, the access-layer devices will perform the traffic classification processing and then use a tag (typically a MPLS tag) that indicates to the service-delivery layer how the traffic is to be treated. The optical switches at the edge of the network then know how to queue and prioritize traffic when congestion occurs. In this manner, decisions do not have to be made regarding how much bandwidth to allocate to each traffic type. Instead, the bandwidth is dynamically shared between the traffic types.

While IP, Optical switching and ATM have different characteristics, they are managed and controlled in similar manners. Trusted paths are established between the router or switch and the management station and trusted channels are established between the routers and switches. Across the trusted path management information is exchanged. Between routers and switches, network control information is exchanged via trusted channels to allow dynamic connection establishment and packet routing. Network control information consists of specific requests and instructions that include destination address, routing controls and signaling information. Examples of control information in the ATM environment include ATM UNI and NNI signaling and PNNI routing. Examples of control information in the IP environment include OSPF, BGP, RSVP, and LDP.

The term node shall be used throughout this document in reference to switches and routers.

2.2 NETWORK SCENARIOS

This protection profile will cover switches and routers operating in 3 different environments.

1) The routers or switches will be owned and managed by the same organization. Figure 1.0, below, depicts an example architecture for this scenario. Personnel who manage the nodes are given a high level of trust. User traffic traversing this closed/internal network is considered sensitive and may be unencrypted.

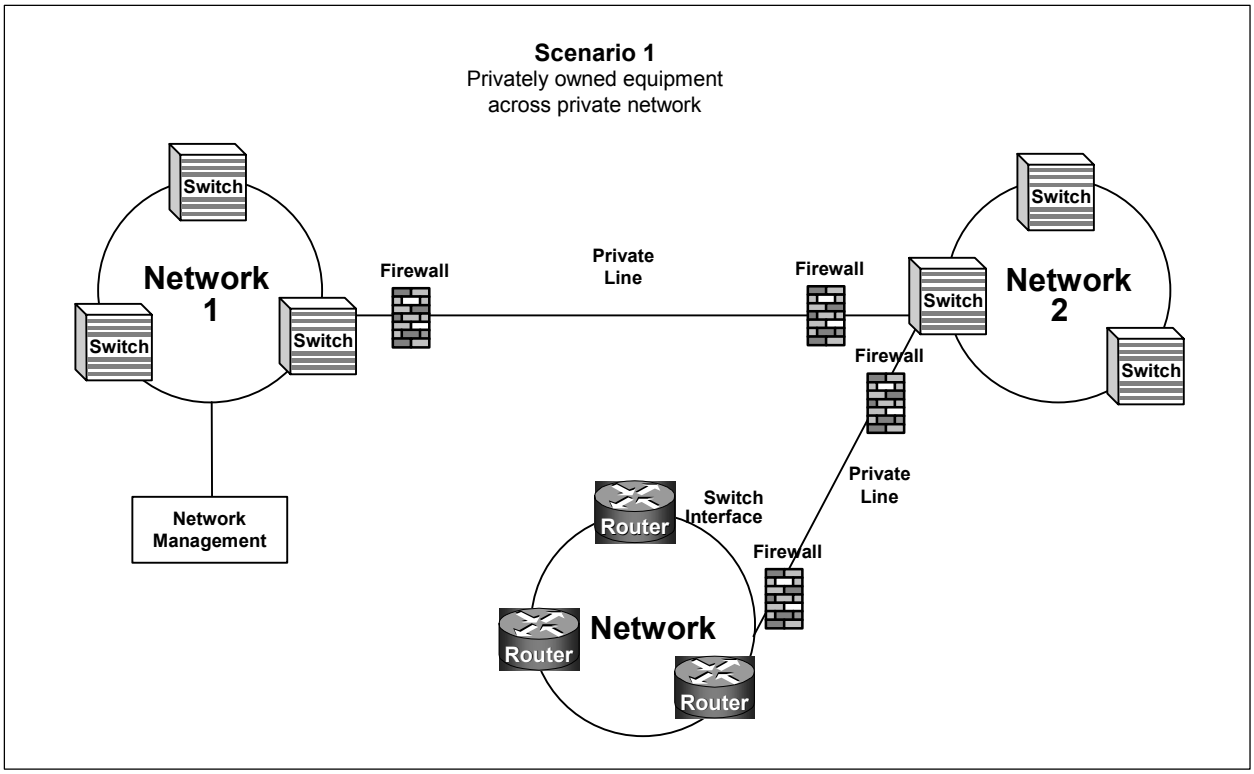

Figure 1.0 – Private Line

2) Equipment is owned by an organization but managed by a network provider or commercial organization. This environment describes nodes that are managed by and could be physically isolated in the network providers' or commercial organizations' facility. Figure 2.1 depicts an organization sending information across leased line connections. Figure 2.2 depicts an organization that utilizes a network providers backbone network to transmit information. The equipment is physically isolated either in a locked cage or a locked room. Access to these areas is controlled as the keys to these areas are only given to the on-site managers. The network provider or commercial organization manages the nodes and the managers are given some level of trust. The nodes carry only that organization's traffic. User traffic traversing the network in this scenario is assumed to be encrypted and sensitive. Control traffic is sensitive and may or may not be encrypted. Management traffic is assumed to be unencrypted.

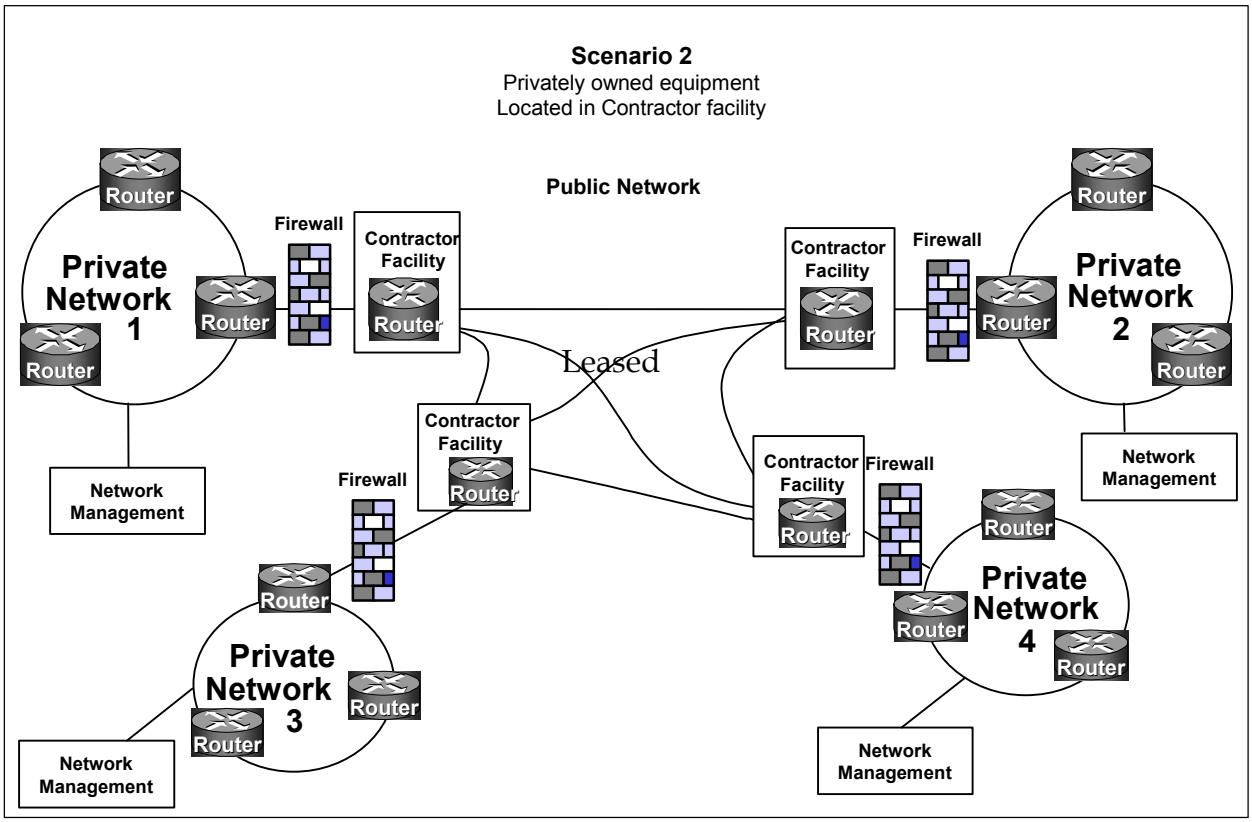

Figure 2.0 – Communication across Leased Lines

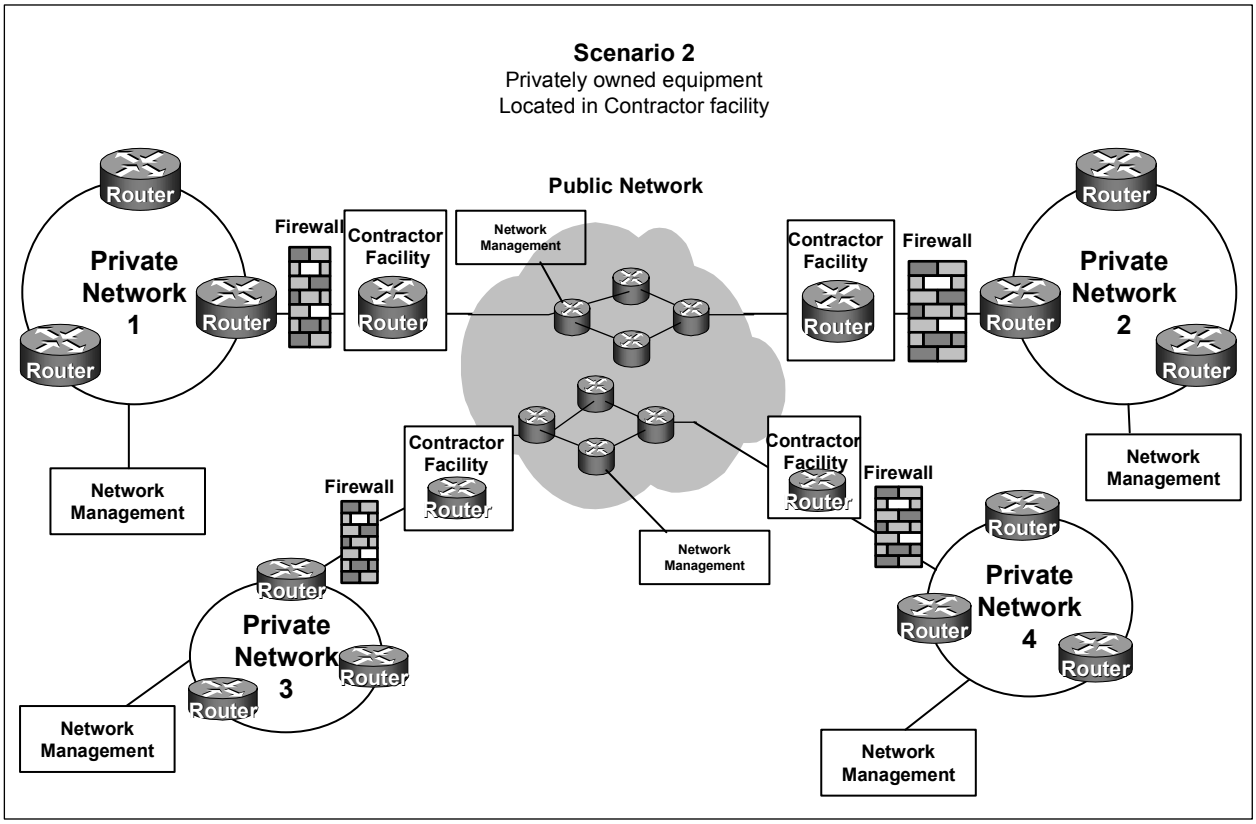

Figure 2.1 – Communication across Public Network

3) An organization purchases service from a provider. The switch or router is owned, managed and resides in the facility of the network provider or commercial organization. Two examples of this type of service arrangement are depicted below in figures 3.0 and 3.1. The managing personnel are given some level of trust. The switches or routers carry a mix of traffic from various organizations therefore the purchasing organization's traffic is assumed to be encrypted and sensitive.

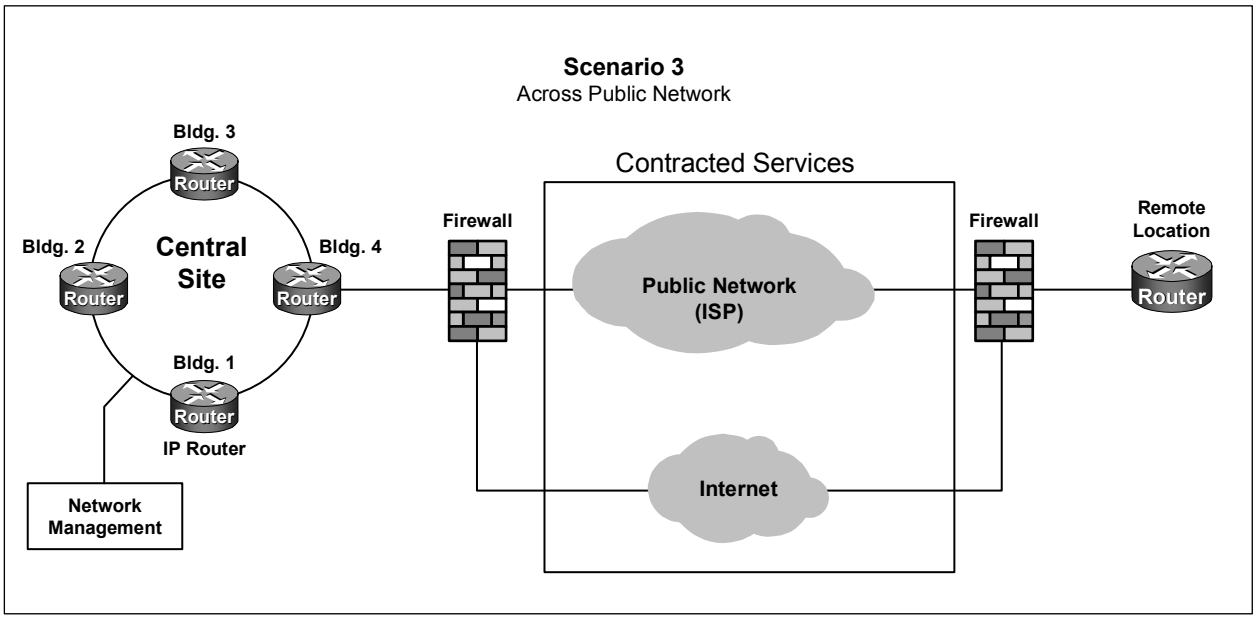

Figure 3.0 – IP Routing across Public Network

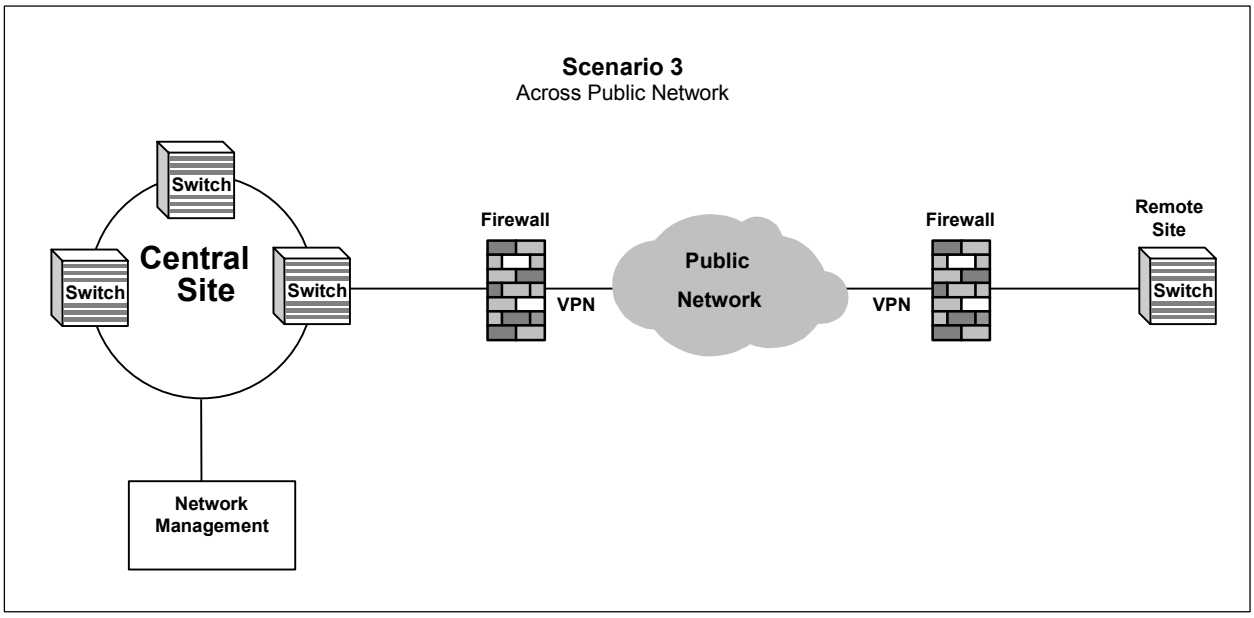

Figure 3.1 – Purchased Switched Services across Public Network

Based on each of the three scenarios presented in the TOE description these network elements have different levels of physical protection. For the first scenario in which the equipment is owned and managed by the same organization, the equipment will be located in a secure area with restricted access by those who have undergone a screening process. The installation and daily maintenance of the equipment will be by highly trusted personnel. For the second scenario where the equipment is owned by one organization but managed and located in a contractor facility, the equipment is located in a locked area, a room or a cage, within the contractor's facility. Only select persons will have access to this area and the building will also have restricted access. The contractor employees may not have necessarily undergone a screening process. The owning organization or a third party may perform the installation and maintenance. In the third scenario where the services are purchased, and traffic is mixed with commercial traffic, the switches and routers are located in a building with restricted access, the floors within the building may also have restricted access. Access to the building is limited to certain network provider employees and contractors who may not have undergone a screening process. Customer organizations do not have access privileges nor do they conduct the maintenance or installation of equipment.

2.3 TOE DESCRIPTION

The Target of Evaluation for this Protection Profile is a switch (e.g., ATM switch or Optical switch) or router, including all cards, ports, software, data and interfaces resident on each. All circuits associated with the switches and routers are part of the TOE, including the management link. While the network management station is an integral component to the network, the network management system is not part of the TOE, nor are any network elements that may be connected to the switch or router, e.g., digital transport (cross-connect) systems, optical transport systems, encryptor devices, etc. However, the TOE must be able to either support encryption or the interface to an encryptor device for user data, and/or management and control information. The intended use of the TOE is to protect the network management and control functions to allow for the reliable transfer of user information across the network with acceptable quality and timeliness of delivery to the intended recipient. Therefore, network control information is considered part of the TOE in this PP. Network management information is also to be considered part of the TOE.

2.4 NETWORK CONTROL AND MANAGEMENT INFORMATION

Network Control information includes routing and signaling information that is shared between switches and routers to coordinate joint operation. The purpose of control information is to control traffic transmission along routes, paths, and channels and to control traffic transmission quality in regards to quality of service (QoS) and discard priority of the cell or packet. The control information is contained within the header of the ATM cell or IP packet and in the case of an IP packet, possibly also in a trailer.

ATM switches use standards such as UNI (3.0, 3.1, and 4.0), NNI, or Q.2931 signalling to pass call control messages between switches to establish a connection. The setup messages contain traffic descriptors and addressing information about each downstream node. Protocols, such as PNNI, OSPF, BGP, RSVP, LDP, etc., are passed between nodes to establish services and reserve resources between nodes. To allow for reliable operation of the network authentication and integrity of control information is necessary. Additionally, routing and signaling information may be considered sensitive as this information can reveal the network topology and provide traffic flow information. When protection of the network topology and traffic flow information is important and necessary, means to retain the confidentiality of routing and signaling information must be employed.

Whereas network control information is mainly focused on configuration, network management information is mainly focused on performance, fault, failure, and accounting. The TOE will be connected to the facility responsible for network management by a management link. This management link will be a trusted path. The

protection of a node can be thought of as protecting the access to the node. Access can take several different forms, therefore the information and assets that require protection include network management data, and network control information.

There are several methods of managing a node. One of the most common methods of managing these devices is called in-band management. Using in-band management the management traffic uses the same communications links and ports as the client traffic. In-band management requires the protocols that include but are not limited to, SNMP, RMON, CMIP, HTTP, Telnet, Rlogin, etc.

Another method of managing nodes is by out-of-band methods. The term out-of-band is used for multiple management mechanisms using a port other than the client port. There are several methods of out-of-band management. First, the node can be managed through a local port. A laptop computer or a dumb terminal, physically adjacent to the node, may be connected to a serial interface port. Second, the node may also be managed by a laptop computer or terminal not physically adjacent to the node and remotely accessed through the PSTN (Public Switched Telephone Network). Third, the switch or router could be accessed through an Ethernet network by a management station that is physically separate from the node (e.g., Telnet, rsh, HTTP, etc).

There are different roles in the management of nodes. All personnel in management roles are assumed to be trusted at some level even though they may not have gone through a screening process. The management facility is a privileged access area with only the network management employees having access privileges. Access to the management link can be restricted based on network address. The majority of roles have limited privileges to perform their job. Roles are defined and can have overlapping and subsets of privileges. There will be a limited number of roles that will have global privileges over the management of the node. Network Performance Management Operators have viewing privileges only, including the authorization to gather and analyze network performance statistics. Network Management Administrators have the same privileges as Network Performance Management Operators and have access to privileged functions such as configuring, provisioning, trouble shooting and monitoring. Network Management Security Administrators perform functions such as load keys, create and modify access control lists, and restrict applications. Therefore, Network Management Security Administrators will have these privileges as well as those of Network Management Administrators.

Additionally, when network services are purchased, an organization may want to monitor the performance of their own traffic to ensure compliance with the service level agreement as it passes through a provider's network. The network provider or commercial organization may conduct network management activities and provide customer network management reports. The customer management report could be provided via the web on a read-only basis with privileged access rights. The reports

could also be pushed to authorized individuals or the capability will exist for authorized individuals to pull reports at will. Traffic performance statistics include but are not limited to capturing, the date, time of day, network usage statistics versus QoS level, amount of traffic sent, amount of traffic received, etc.

2.5 REQUIRED SECURITY FUNCTIONALITY

The desired security capabilities and functionalities of switches and routers include but are not limited to the following:

- Ability to detect and resist attacks against the TOE that could result in the degradation, interruption or denial of service to users.
- The ability of the switch/router to quickly and successfully recover all security functionality after an attempt against the security of the TOE, an interruption of the TOE security function, and after experiencing any down time.
- Re-play protection of the management plane to ensure that an attacker cannot masquerade as an authenticated client to gain access to the TOE by playing back a previously recorded message.
- Re-play protection of the control plane to ensure that an attacker cannot masquerade as an authenticated client to gain access to the TOE by playing back a previously recorded message.
- Integrity and authentication of the management plane to ensure that information is not altered during transmission.
- Integrity and authentication of the control plane to ensure that information is not altered during transmission as well as the ability to recover from routing convergence disagreements when the topology of the network changes.
- Accountability so that organizations and management personnel can be held responsible for all activities initiated.
- Ability to audit management activities, e.g. configuration activities.
- Ability to audit network traffic activities.
- Capability to customize audit reports of specific attributes from all network management and network activities recorded for ease of analysis.
- Authentication and authorization to gain access to end nodes.
- Authentication and authorization for peer node to establish connections to end nodes based on addresses, ports, etc.
- Authentication and authorization of network management personnel to end nodes of the network based on role (Network Performance Management Operators, Network Management Administrators and Network Management Security Administrators).
- Ability to disable features that could otherwise weaken or break security functionality. The default setting for these features must be for the disabled mode. All functions contributing to TOE Security Functions shall be enabled by default.

3.0 TOE SECURITY ENVIRONMENT

This section lists the assumptions, threats, policies and objectives of the TOE security environment.

3.1 SECURE USAGE ASSUMPTIONS

The specific conditions listed below are key assumptions. These assumptions include practical realities and environmental considerations in the development of security requirements.

A.Audit_Review: Review of Audit Information
Audit information is reviewed and analyzed on a periodic basis in accordance with the network security policy.

A.Cryptanalytic: Robust Encryption
Cryptographic methods used in the TOE environment will be resistant to cryptanalytic attacks and be of adequate robustness to protect sensitive data.

A.Environment: Environmental Protection
All equipment complies with environmental standards, e.g. is NEBS compliant at some level, to ensure physical protection and electrical safety against natural disasters. The TOE has adequate backup power sources to ensure that the sudden loss of power does not affect the availability of services or the loss of data.

A.ExpAgent: Expert Threat Agents
The TOE is subject to deliberate attack by experts with advanced knowledge of security principles and concepts employed by the TOE.

A.Physical: Physical Protection
The TOE is located within controlled access facilities that prevent unauthorized physical access by outsiders. The TOE is installed so that it is protected from casual contact by employees (e.g., unintentional harm that could be caused by a person knocking into the cables). Resistance to physical access will vary based on the different environments described in section 2.2.

A.Time_Source: Reliable Time Source
Network resources are connected to a reliable time source. This is necessary for the proper synchronization of transmissions among resources, for reliable time stamps for auditing purposes of traffic, performance, auditing of Network Management Administrator and Network Management Security Administrator activities, etc. There is a secondary back-up time source.

A.Train: Personnel Training
All personnel are properly trained to develop, install, configure and maintain the TOE, TOE security functions and all network components. All personnel follow documented processes and procedures.

3.2 THREATS TO SECURITY

Technology is required to counter the threats that are listed below. Included with countermeasures are detect and respond mechanisms. Even with security measures, a level of risk acceptance will need to be established.

T.Analysis: Traffic Analysis
An attacker collects source and destination addresses, volume of data and time of day that messages are sent.

T.Capture: Unauthorized Network Access to Capture Data
An attacker eavesdrops, taps into the transmission line, or otherwise captures data being transferred on a communications channel.

T.Compromised_Node: Compromised Node
A node becomes compromised, altering TOE configuration files and/or the routing table, causing incorrect operations of the TOE, disabling of TOE security features, and/or re-routing of traffic which could be re-routed through an unauthorized node.

T.Covert: Covert Channels
Covert Channels are used to hide information in any unused fields in order to send information without being monitored.

T.Cryptanalytic: Cryptoanalysis for Theft of Information
An attacker attempts cryptoanalysis on encrypted data in order to recover message content.

T. Denial: Denial of Service
An attacker executes commands, sends more than allowed high priority traffic, or performs other operations that cause undue burden on the network therefore making system resources unavailable to authorized clients, e.g., resulting in service denial.

T.Fail: Component or Power Failure
Failure of one or more system components or a power failure results in the loss of system-critical functionality and system data.

T.Flaw: Flaws in Hardware, Software or Firmware

Flaws in hardware, software or firmware cause vulnerabilities in the TOE and the TSF.

T.Hostile_Admin: Management Personnel Abuse of Network Authorization
A Network Management Administrator or Network Management Security Administrator intentionally abuses granted authorizations to inappropriately access or modify information, e.g. configuration data, audit data, password files, or other mishandling of sensitive data files.

T.Mgmt_Error: Management Error
A person in a network management role makes a security relevant error that results in inappropriate access or modification of information, or inappropriate utilization of resources.

T.Modify: Modification of Protocols
An attacker makes unauthorized modifications, or manipulates protocols (e.g. routing, signalling, etc.) en-route.

T.NtwkMap: Network Mapping
An attacker attempts to map the network - thus obtaining addresses of nodes, routing table information and physical locations.

T.Replay_Attack: Replay Attack
An attacker records a communication session in order to masquerade as an authenticated client to gain access to the TOE by playing back the previously recorded message. Management information could also be recorded and re-played in an attempt to masquerade as an authenticated Network Management Administrator or a Network Management Security Administrator to gain access to network management resources.

T.Spoof: Spoofing Attack
A client masquerades as an authorized person by obtaining a network address in an attempt to gain access to TOE resources. An unauthorized node may attempt to access a network by using a valid network address.

T.Unauth_Mgmt_Access: Unauthorized Access to the Management port
An attacker may access, or a person in a network management role may abuse their privileges and gain access to the management port, either through Telnet, RMON etc., to re-configure the network, cause denial of service to clients, monitor traffic to perform traffic analysis, etc.

3.3 ORGANIZATIONAL SECURITY POLICIES

Organizational security policies are listed below.

P.Accountability: Individual Accountability
Organizations that use the TOE for transmitting information, persons in network management roles and developers shall be held accountable for their actions.

P.Audit _Admin: Audit Management Personnel Data
The network management system shall be able to generate and transmit audit records. Audit records shall be provided & include enough information to determine the Network Management Administrator or the Network Management Security Administrator and the date, time, and actions that occurred during the session. Audit records shall be reviewed on a periodic basis.

P.Authentication: Authentication of Operators and Nodes
The TOE shall support authentication of Network Performance Management Operators, Network Management Administrators, and Network Management Security Administrators. The TOE shall support authentication of peer nodes.

P.Availability: Network Availability
Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.

P.Confidentiality: Information Confidentiality
Statistical data, configuration and connectivity information will remain confidential, both in real-time and as stored data. To aid in retaining confidentiality, the TOE must be able to support a robust cryptographic infrastructure. The TOE must be capable of cryptography or support interfaces to cryptographic devices.

P.Default_Config: Default Configuration
The default configuration settings for the TOE will have all functions that weaken or break TOE security functions disabled. All functions contributing to TOE Security Functions shall be enabled by default.

P.Guidance: Installation and Usage Guidance
Guidance documents will be provided for the secure installation, configuration and maintenance of the switches and routers.

P.Information_Update: TOE Informational Updates
Ensure the integrity of TOE informational documents, known anomalies, patches, upgrades, etc. upon receipt. These documents, patches, upgrades, etc. will be released and distributed on a scheduled timely basis.

P.Integrity: Content Integrity
Management and control information shall retain its content integrity during transmission. All information shall retain its integrity as stored information.

P.Interoperability: Interoperability
The TOE shall be interoperable with switches/routers of other vendors. Standardized, nonproprietary, protocols (routing, signalling, etc.) shall be implemented in the TOE. The vendor may choose to implement some proprietary protocols however, for interoperability the vendor shall also implement standardized protocols in the TOE.

P.Notify: Notification of Failure
The TOE and the TSE will be capable of alerting and providing alarms, e.g. via SNMP3 traps, in the event of a component, firmware, hardware or software failure.

P.Peer: Peer Nodes
Secure nodes will have the ability to accept traffic from trusted and untrusted nodes. Traffic will be filtered between trusted & untrusted nodes to protect information.

P.Procedures: Procedures for Management of Information
Procedures will be in place to restrict the inadvertent disclosure or modification of sensitive information or improper utilization of resources in the TSE. Examples of sensitive information include, but are not limited to, printed material detailing operations procedures, equipment installation procedures, audit files, configuration files, network diagrams, information across physical connections and network test results.

P.Reliable_Transport: Reliable Transport
Protocols specifying reliable transport and error detection mechanisms shall be implemented for network management and control.

P.Survive: Network Survivability & Recovery
Resources shall be able to recover from hostile attempts against security. Resources must also be able to recover from errors that may occur during transmission. The network must be able to be resistant, or recover in a reasonable amount of time from a hardware or software failure. Any circumstances that could result in a partial recovery shall be documented.

P.SysAssur: Hardware, Software, and Firmware Integrity
Features and procedures to validate the integrity and the expected performance of initial and all upgraded versions of hardware, software and firmware shall be provided. Integrity shall be ensured at the time of initial installation and at the time of software upgrades and firmware swap-outs as well.

4.0 SECURITY OBJECTIVES

The following are security objectives for the TOE and the TOE environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

O.Access_Control: Network Access Control
Implement an access control policy. The access control policy will be based on, but not limited to the following, the TOE's role (handling trusted only, untrusted, or a mix of traffic), the TOE's identity (owned by an organization, owned by the network provider and supporting many organizations/clients), source and destination addresses, filtering at the port level (Telnet, SNMP, etc.), etc.

O.Alarm: Alarm Notification for Security Risks
The TOE will be capable of detecting a failure or error with any component, hardware, software, or firmware. The TOE will provide alarming capabilities for notification of security related events and of a failure or error.

O.Cfg_Confidentiality: Network Configuration Confidentiality
Configuration and connectivity information will not be disclosed.

O.Cfg_Integrity: Configuration Integrity
Audit files, configuration, connectivity information, and other information pertaining to the TOE will retain its content integrity. The TOE does not have to be responsible for storing this information.

O.Cfg_Manage: Manage Configuration Data
Implement a plan in which to capture and retain configuration and connection information for each switch and/or router. The plan must assure storage integrity, identification of system connectivity and identification of system components.

O.Ctrl_Channel: Trusted Channel for Control Data
Provide integrity and confidentiality of all control data transferred between peer TOEs. Provide a trusted channel that is distinct from and cannot be confused with other communications. To aid in providing confidentiality, the TOE must be able to support a cryptographic infrastructure. The cryptographic infrastructure will support services

including client registration, key management and segregation of communities of interest.

O.Ctrl_I&A: Control Identification and Authentication
Connectivity will be provided between peer TOEs only upon the identification, authentication and authorization of the requesting and destination addresses in accordance with the access control policy.

O.Detect_Connection: Detection of Unauthorized Connections
The TOE will be able to detect and alert of unauthorized connections.

O.Fail_Secure: Preservation of Secure State for Failures
Preserve the secure state of the system in the event of a component or power failure.

O.Lifecycle: Lifecycle Security
The TOE will be managed and maintained such that its security functions are implemented and preserved throughout its operational lifetime. Upgrades made to the hardware, software or firmware will preserve or enhance current security features without affecting any other TSF.

O.Mgmt_Path: Trusted Path for Management Data
Provide integrity and confidentiality of all management data transferred between the TOE and the network management station. Provide a trusted path that is distinct from and cannot be confused with other communications. To aid in providing confidentiality, the TOE must be able to support a cryptographic infrastructure. The cryptographic infrastructure will support services including client registration, key management and segregation of communities of interest.

O.Patches: Security Fixes and Patches
The TOE will have the latest patches and security fixes installed.

O.Priority_of_Service: Provide Priority of Service
Assign priorities to all traffic streams, even if all priorities are set for best effort. Control access to resources so that lower-quality/priority classes of service do not unduly interfere with or delay higher-quality/priority classes of service.

O.Protect_Addresses: Protect Addresses
The TOE will protect the confidentiality and integrity of the transmitting and receiving authorized organizations' internal addresses. Upon receipt, the TOE will correctly interpret both originating and destination authorized addresses.

O.Protocols: Protocols
Standardized protocols shall be implemented in the TOE to achieve interoperability with switches/routers of other vendors. Protocols shall be implemented in the TOE to provide reliable transport and error detection.

O.Replay_Prevent: Prevent Replay Attacks
The TOE will be capable of rejecting old or duplicate packets in order to protect itself against a replay attack where an unauthorized agent may be masquerading as an authorized agent.

O.Test: Testing of the TOE and TSF
Test plans and procedures will be written and followed to test the TOE and the TSF. Vulnerability testing will be conducted to search for methods of how the TOE Security Policy can be violated. All test methods and results will be documented.

O.Traf_Audit: Audit Traffic Records with Identity
Record in audit records traffic and performance statistics including, but not limited to, the date, time, size of traffic data sent (cells/packets per second, kbps, mbps, etc.), size of traffic data received (cells/packets per second, kbps, mbps, etc.), node identifiers and organization responsible for the transmission of data. Ensure the integrity of all audit records. The TOE does not have to be responsible for storing these traffic audit records.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
Ensure that all network files and configuration parameters of the TOE are replicated. The file backup will occur on a regular basis. The data will be consistent and properly stored in accordance with the network security policy so that file integrity and confidentiality is ensured. The backup files will be sufficient to re-create the configuration of the TOE in order to restore the TOE to proper operation in the event of a failure or security compromise. The network files may be replicated by automatically being backed-up to a second management station on a regular basis.

O.Trusted_Recovery: Trusted Recovery
Ensure the recovery to a secure state, without security compromise, after a discontinuity of operations. Ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the network.

O.Unused_Fields: Unused Fields
Ensure that values for all unused fields within the header are properly set. If these fields are not used they will be blocked or reset.

O.Validation: Validation of HW/SW/FW
Ensure, through features and procedures, the integrity of all hardware, software and

firmware and that all hardware, software and firmware is correctly installed and functioning properly.

4.2 SECURITY OBJECTIVE FOR THE ENVIRONMENT

The following are the Protection Profile security objectives that will be satisfied largely through application of procedural or administrative measures.

OE.Admin_Audit: Audit Records with Identity
The actions of Network Management Administrators and Network Management Security Administrators shall be audited. Audit records will be stored and maintained in accordance with the security policy.

OE.Attr_Mgt: Manage Attributes
The Network Management Security Administrator will manage the access control policy within the network management system to only give authorized network management persons the necessary functional abilities. Management personnel will be able to assume their privileged roles within the network management system only upon proper identification and authentication.

OE.Audit_Review: Review of Audit Records
All Audit records will periodically be reviewed. Network Performance Management Operators will periodically review Network Traffic audit records.

OE.Cryptography: Support of Cryptographic Infrastructure
The TOE must be able to support a cryptographic infrastructure in order to aid in providing confidentiality. The cryptographic infrastructure will support services including client registration, key management and segregation of communities of interest.

OE.Environment: Environmental Protection
Resources shall be developed to provide protection against environmental threats, e.g., fire, earthquake, loss of power, etc.

OE.Guide_Docs: Guidance Documentation
Deter installation, configuration and operating errors by providing installation, configuration, operating, and procedural guidance documentation on a timely basis. Guidance Documentation will also assist personnel in the maintenance of the TOE and TOE security functions.

OE.Mgmt_I&A: Management Identification and Authentication
Management personnel will be able to assume their privileged roles within the network

management system only upon proper identification and authentication.

OE.Personnel: Personnel
Attempt to hire and retain trustworthy and competent personnel. Examples of how these characteristics will be ensured include security lectures, polygraphing, monitoring, misuse detection analysis/auditing, and testing. Personnel shall be initially trained and continuous training shall be provided.

OE.Physical: Physical Protection
Resources shall be physically protected to prevent malicious attacks, unauthorized modification, destruction and theft.

OE.Synchronization: Network Synchronization
The TOE shall be connected to a reliable time source to allow for the proper synchronization of network resources.

5.0 IT SECURITY REQUIREMENTS

This section presents the functional and assurance security requirements for the TOE, and environment that must be satisfied to be compliant with this Protection Profile. These requirements consist of functional components from Part 2 of the Common Criteria. Part 3 of the Common Criteria provides the assurance components required to satisfy the EAL of this Protection Profile, Evaluation Assurance Level 3 (EAL3).

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

5.1.1 Class FAU: Security Audit

5.1.1.1 Audit Data Generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of audit functions;
b) All auditable events for the *basic* level of audit; and
c) For Network Performance Management Operators, Network Management Administrators and Network Management Security Administrators audit: distribution or revocations of access rights and capabilities, changes made by any network management person, time and date of log-in sessions and time and date of actions performed by network management persons.

For network traffic audit: be able to record, at a minimum, source & destination nodes within the backbone, size of transmitted and received traffic, date and time.(FAU_GEN.1.1)

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, other relevant audit events include: receipt of traffic from untrusted sources, acceptance of traffic from untrusted sources, response actions taken to recover from a security related event, elapsed time to recover from a security related event, all components affected by a security related event.(FAU_GEN.1.2)

Dependencies: FPT_STM.1 Reliable time stamps

Application Note:
FAU_GEN.1.2 has an assignment for the ability to audit the event of accepting traffic from untrusted sources. The ability to reject or accept traffic from untrusted sources

should be an option that is configurable in accordance with the local security policy.

5.1.1.2 User Identity Association (FAU_GEN.2)
The TSF shall be able to associate each auditable event with the identity of the user that caused the event.(FAU_GEN.2.1)

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

Refinement:
For this requirement, user shall refer to a person in a network management role for network management audit data or refer to the identity of the TOE for traffic statistic audit generation purposes.

Rationale:
FIA_UID.1: Timing of Identification is a listed dependency, however, for this protection profile FIA_UID.2: User Identification was chosen, as the requirement is for a user (Network Management Administrator or a Network Management Security Administrator) to be identified before any actions can be performed.

5.1.1.3 Audit Review (FAU_SAR.1)

The TSF shall provide designated Network Management Security Administrators with the capability to read all audit data from the audit records.FAU_SAR.1.1
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.FAU_SAR.1.2

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.4 Selective Audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: *object identity, user identity, subject identity and event type*.FAU_SEL.1.1

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

5.1.2 Class FDP: User Data Protection

5.1.2.1 Subset Access Control (FDP_ACC.1)

The TSF shall enforce the access control policy on communication requests.FDP_ACC.1.1

Dependencies: FDP_ACF.1

5.1.2.2 Security Attribute Based Access Control (FDP_ACF.1)

The TSF shall enforce the access control policy to objects based on identification, authentication and authorization to connect to another node that is a member of the communications session.FDP_ACF1.1
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the source TOE address must be identified on the recipient TOE's access control list and authorization must occur prior to receiving messages.FDP_ACF.1.2
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: possession of a valid key, the TOE's role (handle traffic from trusted sources only, or configured to also accept traffic from untrusted sources), time of day, and traffic characteristics (e.g. control information).FDP_ACF.1.3
The TSF shall explicitly deny access of subjects to objects based on the address of the sender.FDP_ACF.1.4

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.1.2.3 Export of User Data with Security Attributes (FDP_ETC.2)

The TSF shall enforce the application of security attributes when exporting user data, controlled under the SFP, outside of the TSC.FDP_ETC.2.1
The TSF shall export the user data with the user data's associated security attributes.FDP_ETC.2.2
The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.FDP_ETC.2.3
The TSF shall enforce the following rules when user data is exported from the TSC: the transmitting TOE must ensure integrity protection.

Dependencies: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control.

5.1.2.4 Subset Information Flow Control (FDP_IFC.1)
The TSF shall enforce the information flow control policy on control information (signaling and routing information) received from untrusted sources.FDP_IFC.1.1

Dependencies: FDP_IFF.1 Simple security attributes

5.1.2.5 Simple Security Attributes (FDP_IFF.1)
The TSF shall enforce the information flow control policy based on the following types of subject and information security attributes: at a minimum the information flow control policy must

1) function in conjunction with the access control policy,
2) be able to recognize the source of control information as being either trusted or untrusted (a trusted source is one that is able to be identified and authenticated and the integrity of the control information is able to be verified),
3) allow for the identification of the originating source of the message.FDP_IFF.1.1

The TSF shall permit an information flow between controlled subjects via a controlled operation if the following rules hold: the source of the message is able to be identified and authenticated by the recipient, and the integrity of the message is verified.FDP_IFF.1.2
The TSF shall enforce the information flow control policy in that control information from trusted sources will be given priority over the control information received from untrusted sources when making routing or re-routing decisions, as in the event of a network failure.FDP_IFF.1.3
The TSF shall provide the following the ability to configure the TSF to implement a policy decision for accepting data from an untrusted source and to audit the receipt of data from an untrusted source and the acceptance of data from an untrusted source.FDP_IFF.1.4
The TSF shall explicitly authorize an information flow based on the following rules:
1) trusted pre-established (static) routes,
2) management information through a trusted path to the network management station.FDP_IFF.1.5
The TSF shall explicitly deny an information flow based on the following rules: in accordance with security policy configuration setting to deny the receipt of data from untrusted sources.FDP_IFF.1.6

Dependencies: FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

Refinement:
FDP_IFF.1.2 states "The TSF shall permit an information flow between a controlled subject and controlled information…" This statement has been refined to read "The TSF shall permit an information flow between controlled subjects…"

5.1.2.4 Import of User Data with Security Attributes (FDP_ITC.2)
The TSF shall enforce the use of identity based access control lists, verification of possession of proper key material, verification of integrity check, or the recognition of source addresses when importing user data, controlled under the SFP, from outside of the TSC.FDP_ITC.2.1
The TSF shall use the security attributes associated with the imported user data.FDP_ITC.2.2
The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.FDP_ITC.2.3
The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.FDP_ITC.2.4
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [ST assignment].FDP_ITC.2.5

Dependencies: FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset information flow control
FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path
FPT_TDC.1 Inter-TSF basic TSF data consistency

5.1.2.5 Data Exchange Integrity (FDP_UIT.1)

The TSF shall enforce the information control policy to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion and replay* errors.FDP_UIT.1.1
The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion or replay* has occurred.FDP_UIT.1.2

Dependencies: FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset information flow control
FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path
FTP_TRP.1 Trusted path

Application Note:
For the purpose of this Protection Profile, the term user data used in this requirement, FDP_UIT.1, can be defined as control information or management information.

5.1.2.5 Source Data Exchange Recovery (FDP_UIT.2)

The TSF shall enforce the request to perform frame check sequence, cyclic redundancy check, traffic shaping, anti-replay, and to completely duplicate all network management data files to a separate back-up source. These requests are necessary to be able to recover from ordering changes of packets, replayed packets, incomplete data transfer, dropped packets, network congestion and a failure with the primary network management system with the help of the source Trusted IT Product.FDP_UIT.2.1

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow Control
FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted Path

Refined by adding:
The requirement states that a trusted IT product assists in data exchange recovery. This requirement is refined so that the other product is another switch or router.

5.1.3 Class FIA: Identification and Authentication

5.1.3.1 User Authentication Before any Action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.FIA_UAU.2.1

Dependencies: FIA_UID.1 Timing of identification

Application Note:
For this requirement the term 'user' is to refer to the source of the transmitted information. If the source of the information is identified as being from an 'untrusted' source then the configurable option of the TOE, in conjunction with the information flow control policy and the access control policy, will allow or disallow the receipt of the information.

5.1.3.2 User Identification (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of the user.(FIA_UID.2.1)

Application Note:
For this requirement the term 'user' is to refer to the source of the transmitted

information. If the source of the information is identified as being from an 'untrusted' source then the configurable option of the TOE, in conjunction with the information flow control policy and the access control policy, will allow or disallow the receipt of the information.

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

5.1.4.1 Management of Security Functions Behavior (FMT_MOF.1)

The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions of the TOE at the time of installation and throughout the lifecycle, TOE security fixes/patches, selecting auditable events, managing user accounts, managing the audit logs, managing the access control policy, managing the information flow control policy, TOE connection to a reliable time source, maintenance of TOE resources including backup and recovery of TOE data files to the Network Management Security Administrator roles.

The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions of TOE configuration and maintenance of TOE resources to the Network Management Administrator responsible for establishing and configuring connections.FMT_MOF.1.1

Dependencies: FMT_SMR.1 Security roles

Application Note:
While the dependency for FMT_MOF.1 is FMT_SMR.1, FMT_SMR.2 was chosen to specify the rules that control the relationship between Network Management Security Administrator and Network Performance Management Operator and Network Management Administrator roles.

5.1.4.2 Management of Security Attributes (FMT_MSA.1)

The TSF shall enforce the access control policy to restrict the ability to *change the default settings, create, modify, delete* the security attributes of selecting auditable events, managing audit logs, network management system access control lists and accounts, network user access control lists and accounts to Network Management Security Administrator roles.

The TSF shall enforce the access control policy to restrict the ability to *change the default settings, create, modify, delete* the security attributes of network user access control lists

and accounts to Network Management Administrators .

The TSF shall enforce the access control policy to restrict the ability to monitor and gather network performance attributes and the security attributes for monitoring and analyzing traffic performance to Network Performance Management Operators, Network Management Administrators and Network Management Security Administrators.FMT_MSA.1.1

Dependencies: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information Flow Control
FMT_SMR.1 Security roles

Application Note:
While the dependency for FMT_MSA.1 is FMT_SMR.1, FMT_SMR.2 was chosen to specify the rules that control the relationship between Network Management Security Administrator and Network Performance Management Operator and Network Management Administrator roles.

5.1.4.3 Static Attribute Initialization (FMT_MSA.3)

The TSF shall enforce the access control policy to provide *restrictive* default values for security attributes that are used to enforce the SFP.FMT_MSA.3.1
The TSF shall allow the Network Management Administrator or the Network Management Security Administrator responsible for establishing and configuring connections to specify alternative initial values to override the default values when an object or information is created.FMT_MSA.3.2

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.4.4 Management of TSF Data (FMT_MTD.1)

The TSF shall restrict the ability to *change the default and query* the currently specified fields of the network management audit data, and network traffic audit data to Network Management Security Administrators.FMT_MTD.1.1

The TSF shall restrict the ability to *change the default and query* the currently specified fields of the network traffic audit data to Network Management Administrators.FMT_MTD.1.1

The TSF shall restrict the ability to *query* the currently specified fields of the network traffic audit data to Network Performance Management Operators.FMT_MTD.1.1

Dependencies: FMT_SMR.1 Security Roles

Application Note:
While the dependency for FMT_MTD.1 is FMT_SMR.1, FMT_SMR.2 was chosen to specify the rules that control the relationship between Network Management Security Administrator and Network Performance Management Operator and Network Management Administrator roles.

5.1.4.5 Restrictions on Security Roles (FMT_SMR.2)

The TSF shall maintain the role of Network Management Security Administrator.FMT_SMR.2.1

The TSF shall be able to associate users with roles.FMT_SMR.2.1

The TSF shall ensure that the condition is satisfied that a Network Performance Management Operator or Network Management Administrator cannot assume the role of a Network Management Security Administrator.FMT_SMR.2.3

Dependencies: FIA_UID.1 Timing of identification

Application Note:
While the dependency for this requirement is FIA_UID.1, FIA_UID.2 was chosen since no TSF actions shall be taken before identification of the Network Management Administrator or the Network Management Security Administrator.

5.1.5 Class FPT: Protection of the TSF

5.1.5.1 Abstract Machine Testing (FPT_AMT.1)

The TSF shall run a suite of tests *during initial start-up and at the request of* the Network Management Security Administrator or the Network Management Administrator to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.FPT_AMT.1.1

Dependencies: No dependencies

Application Note:
The abstract machine refers to any of the hardware, firmware and/or software of the network management functions performed by the TOE.

5.1.5.2 Failure with Preservation of Secure State (FPT_FLS.1)

The TSF shall preserve a secure state when the following types of failures occur: hardware component failure, short power interruption.FPT_FLS.1.1

Dependencies: ADV_SPM.1 Informal TOE security policy model

5.1.5.3 Inter-TSF Confidentiality during Transmission (FPT_ITC.1)

The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.FPT_ITC.1.1

Dependencies: No dependencies

5.1.5.4 Inter-TSF Detection of Modification (FPT_ITI.1)

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: the strength must be conformant to or greater than the strength offered by MD5.FPT_ITI.1.1
The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform a retransmission of data and generate an audit record if modifications are detected.FPT_ITI.1.2

Dependencies: No dependencies

5.1.5.5 Passive Detection of Physical Attack (FPT_PHP.1)

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.FPT_PHP.1.1
The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.FPT_PHP.1.2

Dependencies: FMT_MOF.1 Management of security functions behavior

5.1.5.6 Automated Recovery without Undue Loss (FPT_RCV.3)

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.FPT_RCV.3.1
For backup power supply, redundant processors, network management system error or failure, component (card, port) failure, the TSF shall ensure the return of the TOE to a secure state using automated procedures.FPT_RCV.3.2

The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [ST assignment] for loss of TSF data or objects within the TSC.FPT_RCV.3.3
The TSF shall provide the capability to determine the objects that were or were not capable of being recovered. FPT_RCV.3.4

Dependencies: FPT_TST.1 TSF testing
AGD_ADM.1 Administrator guidance
ADV_SPM.1 Informal TOE security policy model

5.1.5.7 Function Recovery (FPT_RCV.4)

The TSF shall ensure that security functions such as, but not limited to, APS (Automatic Protection Switching), switch-over to redundant processor, switch-over to backup power supply, preservation of information transfer connection, cyclic redundancy check, frame check sequence, anti-replay, and failure scenarios such as, hardware component failure, loss of power, software error/failure, system processor failure, network management system failure, downed circuit, or component failure have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.FPT_RCV.4.1

Dependencies: ADV_SPM.1 Informal TOE security policy model

5.1.5.8 Replay Detection (FPT_RPL.1)

The TSF shall detect replay for the following entities: messages (e.g., management and control), security negotiation messages, specific characteristics (nonce, timestamps, hash, keys, etc.) that are identified with a cell/packet transfer.FPT_RPL.1.1
The TSF shall perform auditing, confirmation request from the legitimate source for the replay, block communication from the source of origin, send traps to test the line and scan for unauthorized connections when replay is detected.FPT_RPL.1.2

Dependencies: No dependencies

5.1.5.9 Reliable Time Stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

Dependencies: No dependencies

5.1.5.10 Inter-TSF Basic TSF Data Consistency (FPT_TDC.1)

The TSF shall provide the capability to consistently interpret network audit information, control information and security parameters when shared between the TSF

and another trusted IT product.FPT_TDC.1.1
The TSF shall use authenticated protocols (in the Security Target) as specified by the developer when interpreting the TSF data from another trusted IT product. FPT_TDC.1.2

Dependencies: No dependencies

5.1.5.11 TSF Testing (FPT_TST.1)

The TSF shall run a suite of self tests *during initial start-up and at the request of the* Network Management Security Administrator or Network Management Administrators to demonstrate the correct operation of the TSF.FPT_TST.1.1
The TSF shall provide authorized users with the capability to verify the integrity of TSF data.FPT_TST.1.2
The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.FPT_TST.1.3

Dependencies: FPT_AMT.1 Abstract machine testing

5.1.6 Class FRU: Resource Utilization

5.1.6.1 Degraded Fault Tolerance (FRU_FLT.1)

The TSF shall ensure the operation of automatically switching to the back-up component or power-supply, secure information transfers, connection preservation of information transfers, proper routing of traffic, proper internal processing of cells/packets, traffic shaping, preservation of the subscribed quality/priority of service for traffic, dropping corrupted data and auditing the event while continuing proper network operation with pre-attack control information when the following failures occur: hardware failure, software error, line failure, malicious modification of control and management information en-route, buffer overflow, extreme network congestion, natural disaster (earthquake, flood, etc.), short power interruption.FRU_FLT.1.1

Dependencies: FPT_FLS.1 Failure with preservation of secure state

5.1.6.2 Full Priority of Service (FRU_PRS.2)

The TSF shall assign a priority to each subject in the TSF.FRU_PRS.2.1
The TSF shall ensure that each access to all shareable resources shall be mediated on the basis of the subjects assigned priority.FRU_PRS.2.2

Dependencies: No dependencies

Application Note:
For this requirement, 'subject' shall refer to the set of performance characteristics for a connection. Performance characteristics can be measured in transmission rate, error rates, latency, and other characteristics.

5.1.7 Class FTA: TOE Access

5.1.7.1 TOE Session Establishment (FTA_TSE.1)

The TSF shall be able to deny session establishment based on node identity, received authentication data, originating source identified as being untrusted, role, address, time of day (maintenance windows, or when proper monitoring procedures may not be in place), or based on the security status.FTA_TSE.1.1

Dependencies: No dependencies

5.1.8 Class FTP: Trusted Path/Channels

5.1.8.1 Inter-TSF Trusted Channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.FTP_ITC.1.1
The TSF shall permit *the TSF, the remote trusted IT product* to initiate communication via the trusted channel.FTP_ITC.1.2
The TSF shall initiate communication via the trusted channel for the transmission of control information and transfer of security attributes.FTP_ITC.1.3

Dependencies: No dependencies

Refinement:
FTP_ITC.1.1 states that "…and protection of the channel data from modification or disclosure." For the purpose of this protection profile, protecting channel data from *disclosure* is optional for the implementation of this requirement.

Application Note:
1) The remote trusted IT product refers to a switch or router.
2) A Trusted Channel provides a means for clients to perform functions through an assured connection from TOE to TOE. A trusted channel is used to transmit control

information for messages and is also desired for client actions such as identification and authentication. A trusted channel is a routing channel, a signaling channel, or a remote user connection (e.g., telnet, Rlogin, etc.) and is also referred to as a control channel.

5.1.8.2 Trusted Path (FTP_TRP.1)

The TSF shall provide a communication path between itself and *local and remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.FTP_TRP.1.1
The TSF shall permit *local and remote users* to initiate communication via the trusted path.FTP_TRP.1.2
The TSF shall require the use of the trusted path for *initial authentication* and transmission of network management information.FTP_TRP.1.3

Dependencies: No dependencies

Refinement:
1) FTP_TRP.1.1 states that "…and protection of the communicated data from modification or disclosure." For the purpose of this protection profile, protecting communicated data from *disclosure* is optional for the implementation of this requirement.

2) This requirement has been refined for FTP_TRP.1.1 and FTP_TRP.1.2 to include all ***authorized*** local and remote users (clients). All ***authorized*** local and remote clients shall be permitted to initiate communication via the trusted path.

Application Note:
A Trusted Path is a communication path for which exchanges may be initiated by either side of the channel and both ends of the path are identifiable. A trusted path contains identified subsets of TSF data and commands. For the purpose of this protection profile a trusted path is the network management link. Therefore, one end of the path is the network management station and the other end is the switch or router that is being managed.

5.2 TOE SECURITY ASSURANCE REQUIREMENTS

5.2.1 Class ACM: Configuration Management

5.2.1.1 Partial CM Automation (ACM_AUT.1)

The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.ACM_AUT.1.1C
The developer shall use a CM system.ACM_AUT.1.1D
The CM system shall provide an automated means to support the generation of the TOE.ACM_AUT.1.2C
The developer shall provide a CM plan.ACM_AUT.1.2D
The CM plan shall describe the automated tools used in the CM system.ACM_AUT.1.3C
The CM plan shall describe how the automated tools are used in the CM system.ACM_AUT.1.4C

Dependencies: ACM_CAP.3 Authorization controls

5.2.1.2 Authorization Controls (ACM_CAP.3)

The reference for the TOE shall be unique to each version of the TOE.ACM_CAP.3.1C
The developer shall provide a reference for the TOE.ACM_CAP.3.1D
The TOE shall be labeled with its reference.ACM_CAP.3.2.C
The developer shall use a CM system.ACM_CAP.3.2D
The CM documentation shall include a configuration list and a CM plan.ACM_CAP.3.3C
The developer shall provide CM documentation.ACM_CAP.3.3D
The configuration list shall describe the configuration items that comprise the TOE.ACM_CAP.3.4C
The CM documentation shall describe the method used to uniquely identify the configuration items.ACM_CAP.3.5C
The CM system shall uniquely identify all configuration items.ACM_CAP.3.6C
The CM plan shall describe how the CM system is used.ACM_CAP.3.7C
The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.ACM_CAP.3.8C
The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.ACM_CAP.3.9C
The CM system shall provide measures such that only authorized changes are made to the configuration items.ACM_CAP.3.10C

Dependencies: ACM_SCP.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

Application Note:
The term 'reference' could refer to a version number, naming scheme, etc.

5.2.1.3 TOE CM Coverage (ACM_SCP.1)

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.ACM_SCP.1.1C
The developer shall provide CM documentation.ACM_SCP.1.1D
The CM documentation shall describe how configuration items are tracked by the CM system.ACM_SCP.1.2C

Dependencies: ACM_CAP.3 Authorization controls

5.2.2 Class ADO: Delivery and Operation

5.2.2.1 Delivery Procedures (ADO_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.ADO_DEL.1.1C
The developer shall document procedures for delivery of the TOE or parts of it to the user.ADO_DEL.1.1D
The developer shall use the delivery procedures.ADO_DEL.1.2D

Dependencies: No dependencies

5.2.2.2 Installation, Generation, and Start-up Procedures (ADO_IGS.1)

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.ADO_IGS.1.1C
The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.ADO_IGS.1.1D

Dependencies: AGD_ADM.1 Administrator guidance

5.2.3 Class ADV: Development

5.2.3.1 Fully Defined External Interfaces (ADV_FSP.2)

The functional specification shall describe the TSF and its external interfaces using an informal style.ADV_FSP.2.1C
The developer shall provide a functional specification.ADV_FSP.2.1D
The functional specification shall be internally consistent.ADV_FSP.2.2C
The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.ADV_FSP.2.3C
The functional specification shall completely represent the TSF.ADV_FSP.2.4C
The functional specification shall include rationale that the TSF is completely represented.ADV_FSP.2.5C

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Rationale:
While ADV_FSP.1 is the assurance level of EAL3, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.3.2 Security Enforcing High-Level Design (ADV_HLD.2)

The presentation of the high-level design shall be informal.ADV_HLD.2.1C
The developer shall provide the high-level design of the TSF.ADV_HLD.2.1D
The high-level design shall be internally consistent.ADV_HLD.2.2C
The high-level design shall describe the structure of the TSF in terms of subsystems.ADV_HLD.2.3C
The high-level design shall describe the security functionality provided by each subsystem of the TSF.ADV_HLD.2.4C
The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.ADV_HLD.2.5C
The high-level design shall identify all interfaces to the subsystems of the TSF.ADV_HLD.2.6C
The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.ADV_HLD.2.7C
The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages,

as appropriate.ADV_HLD.2.8C
The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. ADV_HLD.2.9C

Dependencies: ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

Rationale:
While ADV_FSP.1 is the assurance level of EAL3 and a dependency for this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.3.3 Informal Correspondence Demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.ADV_RCR.1.1C
The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.ADV_RCR.1.1D

Dependencies: No dependencies

5.2.3.4 Informal TOE Security Policy Model (ADV_SPM.1)

The TSP model shall be informal.ADV_SPM.1.1C
The developer shall provide a TSP model.ADV_SPM.1.1D
The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.ADV_SPM.1.2C
The developer shall demonstrate correspondence between the functional specification and the TSP model.ADV_SPM.1.2D
The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.ADV_SPM.1.3C
The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.ADV_SPM.1.4C

Dependencies: ADV_FSP.1 Informal functional specification

Rationale:
1) ADV_SPM is not required for EAL 3. ADV_SPM.1 is a dependency of FPT_FLS.1 – Failure with preservation of secure state, FPT_RCV.3 – Automated recovery without

undue loss, and FPT_RCV.4 – Function recovery.

2) While ADV_FSP.1 is the assurance level of EAL3 and a dependency for this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.4 Class AGD: Guidance Documents

5.2.4.1 Administrator Guidance (AGD_ADM.1)

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.AGD_ADM.1.1C
The developer shall provide administrator guidance addressed to system administrative personnel.AGD_ADM.1.1D
The administrator guidance shall describe how to administer the TOE in a secure manner.AGD_ADM.1.2C
The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.AGD_ADM.1.3C
The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.AGD_ADM.1.4C
The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.AGD_ADM.1.5C
The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.AGD_ADM.1.6C
The administrator guidance shall be consistent with all other documentation supplied for evaluation.AGD_ADM.1.7C
The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.AGD_ADM.1.8C

Dependencies: ADV_FSP.1

Rationale:
While ADV_FSP.1 is the assurance level of EAL3 and a dependency for this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.4.2 User Guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. AGD_USR.1.1C

The developer shall provide user guidance.AGD_USR.1.1D
The user guidance shall describe the use of user-accessible security functions provided by the TOE.AGD_USR.1.2C
The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.AGD_USR.1.3C
The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.AGD_USR.1.4C
The user guidance shall be consistent with all other documentation supplied for evaluation.AGD_USR.1.5C
The user guidance shall describe all security requirements for the IT environment that are relevant to the user.AGD_USR.1.6C

Dependencies: ADV_FSP.1

Application Note:
The user in this requirement is not the party responsible for originating traffic. The persons responsible for device operations, a role that may be a subset of the level of Network Management Administrator, is the 'user' in this requirement, AGD_USR.1.

Rationale:
While ADV_FSP.1 is the assurance level of EAL3 and a dependency for this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.5 Class ALC: Life Cycle Support

5.2.5.1 Identification of Security Measures (ALC_DVS.1)

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.ALC_DVS.1.1C
The developer shall produce development security documentation.ALC_DVS.1.1D
The development security documentation shall provide evidence that these security

measures are followed during the development and maintenance of the TOE.ALC_DVS.1.2C

Dependencies: No dependencies

5.2.5.2 Systematic Flaw Remediation (ALC_FLR.3)

The flaw remediation procedure documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.ALC_FLR.3.1C
The developer shall document the flaw remediation procedures.ALC_FLR.3.1D
The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.ALC_FLR.3.2C
The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.ALC_FLR.3.2D
The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.ALC_FLR.3.3C
The developer shall designate one or more specific points of contact for user reports and inquiries about security issues involving the TOE.ALC_FLR.3.3D
The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.ALC_FLR.3.4C
The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.ALC_FLR.3.5C
The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.ALC_FLR.3.6C
The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.ALC_FLR.3.7C

Dependencies: No dependencies

Rationale:
ALC_FLR is not required for any assurance level. ALC_FLR.3 is included so that flaws are tracked and corrected and that information about security flaws are distributed.

5.2.5.3 Well-Defined Development Tools (ALC_TAT.1)

All development tools used for implementation shall be well-defined.ALC_TAT.1.1C
The developer shall identify the development tools being used for the TOE.ALC_TAT.1.1D
The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.ALC_TAT.1.2C

The developer shall document the selected implementation-dependent options of the development tools.ALC_TAT.1.2D
The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.ALC_TAT.1.3C

Dependencies: ADV_IMP.1 Subset of the implementation of the TSF

Rationale:
This assurance is not required to satisfy EAL 3. ALC_TAT.1 is included for the identification of well-defined development tools. Development tools include but are not limited to compilers, simulators, and specialized testing tools. Development tools also include well-defined standards, protocols, RFC's, as published by standards bodies.

5.2.6 Class AMA: Maintenance of Assurance

5.2.6.1 Assurance Maintenance Plan (AMA_AMP.1)

The AM Plan shall contain or reference a brief description of the TOE, including the security functionality it provides.AMA_AMP.1.1C
The developer shall provide an AM Plan.AMA_AMP.1.1D
The AM Plan shall identify the certified version of the TOE, and shall reference the evaluation results.AMA_AMP.1.2C
The AM Plan shall reference the TOE component categorization report for the certified version of the TOE.AMA_AMP.1.3C
The AM Plan shall define the scope of changes to the TOE that are covered by the plan.AMA_AMP.1.4C
The AM Plan shall describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.AMA_AMP.1.5C
The AM Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE. AMA_AMP.1.6C
The AM Plan shall identify the individual(s) who will assume the role of developer security analyst for the TOE.AMA_AMP.1.7C
The AM Plan shall describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.AMA_AMP.1.8C
The AM Plan shall describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.AMA_AMP.1.9C
The AM Plan shall justify why the identified developer security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all

applicable assurance requirements for the certified version of the TOE.AMA_AMP.1.10C
The AM Plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation.AMA_AMP.1.11C

Dependencies: ACM_CAP.2
ALC_FLR.1 Basic flaw remediation
AMA_CAT.1 TOE component categorization report

Rationale:
1) The Maintenance of Assurance class is not required to achieve any EAL. AMA_AMP.1 is included to assure that the developer discloses current plans for any new releases of the TOE. AMA_AMP.1 will also ensure that the TOE will continue to meet its security target so that changes to the TOE will include the discovery of new threats or vulnerabilities.

2) AMA_CAT.1 – TOE component categorization report is a dependency of AMA_AMP.1, however is not included as a requirement for this protection profile. The requirement to categorize the components of the TOE according to their relevance to security can be performed at the discretion of the developer.

5.2.6.2 Evidence of Maintenance Process (AMA_EVD.1)

The AM documentation shall include a configuration list and a list of identified vulnerabilities in the TOE.AMA_EVD.1.1C
The developer security analyst shall provide AM documentation for the current version of the TOE.AMA_EVD.1.1D
The configuration list shall describe the configuration items that comprise the current version of the TOE.AMA_EVD.1.2C
The AM documentation shall provide evidence that the procedures documented or referenced in the AM Plan are being followed.AMA_EVD.1.3C
The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.AMA_EVD.1.4C

Dependencies: AMA_AMP.1 Assurance maintenance plan
AMA_SIA.1 Sampling of security impact analysis

Rationale:
1) The Maintenance of Assurance (AMA) class is not required to achieve any EAL.

AMA_EVD.1 is in conjunction with AMA_AMP.1 to ensure that the assurance maintenance procedures in the assurance maintenance plan are being followed.

5.2.6.3 Examination of Security Impact Analysis (AMA_SIA.2)

The security impact analysis shall identify the certified TOE from which the current version of the TOE was derived.AMA_SIA.2.1C
The developer security analyst shall, for the current version of the TOE, provide a security impact analysis that covers all changes affecting the TOE as compared with the certified version.AMA_SIA.2.1D
The security impact analysis shall identify all new and modified TOE components that are categorized as TSP-enforcing.AMA_SIA.2.2C
The security impact analysis shall, for each change affecting the security target or TSF representations, briefly describe the change and any effects it has on lower representation levels.AMA_SIA.2.3C
The security impact analysis shall, for each change affecting the security target or TSF representations, identify all IT security functions and all TOE components categorised as TSP-enforcing that are affected by the change.AMA_SIA.2.4C
The security impact analysis shall, for each change which results in a modification of the implementation representation of the TSF or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TSF continues to be correctly implemented following the change.AMA_SIA.2.5C
The security impact analysis shall, for each applicable assurance requirement in the configuration management (ACM), life cycle support (ALC), delivery and operation (ADO) and guidance documents (AGD) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact on assurance.AMA_SIA.2.6C
The security impact analysis shall, for each applicable assurance requirement in the vulnerability assessment (AVA) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable. AMA_SIA.2.7C

Dependencies: AMA_CAT.1 TOE component categorization report

Rationale:
1) The Maintenance of Assurance class is not required to achieve any EAL. AMA_SIA.2 is included for assurance that even though changes have been made to the TOE, security functions have been maintained. A security impact analysis will provide this assurance.

2) AMA_CAT.1 – TOE component categorization report is a dependency of AMA_AMP.1, however is not included as a requirement for this protection profile. The requirement to categorize the components of the TOE according to their relevance to

security can be performed at the discretion of the developer.

5.2.7 Class ATE: Tests

5.2.7.1 Analysis of Coverage (ATE_COV.2)

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.ATE_COV.2.1C
The developer shall provide an analysis of the test coverage.ATE_COV.2.1D
The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation are complete. ATE_COV.2.2C

Dependencies: ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Rationale:
While ADV_FSP.1 is the assurance level of EAL3 and a dependency for this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.7.2 Testing: High-Level Design (ATE_DPT.1)

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.ATE_DPT.1.1C
The developer shall provide the analysis of the depth of testing.ATE_DPT.1.1D

Dependencies: ADV_HLD.1 Descriptive high-level design
ATE_FUN.1 Functional testing

Application Note:
While ADV_HLD.1 is a dependency, ADV_HLD.2 is the assurance level required for this protection profile and for EAL3.

5.2.7.3 Functional Testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.ATE_FUN.1.1C
The developer shall test the TSF and document the results.ATE_FUN.1.1D
The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.ATE_FUN.1.2C
The developer shall provide test documentation.ATE_FUN.1.2D
The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.ATE_FUN.1.3C
The expected test results shall show the anticipated outputs from a successful execution of the tests.ATE_FUN.1.4C
The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.ATE_FUN.1.5C

Dependencies: No dependencies

5.2.7.4 Independent Testing - Complete (ATE_IND.2)

The TOE shall be suitable for testing.ATE_IND.2.1C
The developer shall provide the TOE for testing.ATE_IND.2.1D
The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ATE_IND.2.2C

Dependencies: ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
ATE_FUN.1 Functional testing

Rationale:
While ADV_FSP.1 is the assurance level of EAL3 and a dependency of this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.8 Class AVA: Vulnerability Assessment

5.2.8.1- Examination of Guidance (AVA_MSU.1)

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.AVA_MSU.1.1C
The developer shall provide guidance documentation. AVA_MSU.1.1D
The guidance documentation shall be complete, clear, consistent and reasonable.AVA_MSU.1.2C
The guidance documentation shall list all assumptions about the intended environment.AVA_MSU.1.3C
The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).AVA_MSU.1.4C

Dependencies: ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Rationale:
While ADV_FSP.1 is the assurance level of EAL3 and a dependency for this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.8.2 Strength of TOE Security Function Evaluation (AVA_SOF.1)

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.AVA_SOF.1.1C
The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.AVA_SOF.1.1D
For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.AVA_SOF.1.2C

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design

Rationale:
1) ADV_HLD.1 is a dependency for this requirement. This protection profile requires ADV_HLD.2, which is also required for EAL3.

2) While ADV_FSP.1 is the assurance level of EAL3 and a dependency of this requirement, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

5.2.8.3 Developer Vulnerability Analysis (AVA_VLA.1)

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.AVA_VLA.1.1C
The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.AVA_VLA.1.1D
The developer shall document the disposition of obvious vulnerabilities.AVA_VLA.1.2D

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Rationale:
1) ADV_HLD.1 is a dependency for this requirement. This protection profile requires ADV_HLD.2, which is also required for EAL3.

2) While ADV_FSP.1 is the assurance level of EAL3, ADV_FSP.2 was chosen for the assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details supporting thorough testing of the TOE and assessment of vulnerabilities.

6.0 RATIONALE

Rationale for the evidence presented in this Protection Profile is provided in this section. This section ensures that this Protection Profile is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of security countermeasures within the security environment.

Section 6.1 addresses assumption, policy and threat coverage by security objectives

Section 6.2 addresses security objectives coverage by requirements

Section 6.3 addresses the complete and cohesive set of requirements for this PP

Section 6.4 addresses the adequacy of the Assurance Requirements (EAL3 Augmented) chosen for this Protection Profile.

6.1 SECURITY OBJECTIVE RATIONALE

This section contains mapping tables providing evidence of complete coverage. Following the tables are individual arguments for each Policy and Threat that is covered.

Table 6-1 Mapping the TOE Security Environment to Security Objectives

Security Objectives for the TOE	
Policy/Threat/Assumptions	**Security Objectives**
A.ExpAgent	O.Access_Control, O.Ctrl_Channel, O.Ctrl_I&A, O.Detect_Connection, O.Mgmt_Path, O.Protect_Addresses, O.Replay_Prevent, O.Traf_Audit, O.Trust_Backup, O.Unused_Fields
A.Time_Source	O.Traf_Audit

Policy/Threat/Assumptions	Security Objectives
P.Accountability	O.Ctrl_I&A, O.Lifecycle, O.Traf_Audit
P.Authentication	O.Access_Control, O.Ctrl_I&A
P.Availability	O.Access_Control, O.Alarm, O.Fail_Secure, O.Priority_Of_Service, O.Replay_Prevent
P.Confidentiality	O.Cfg_Confidentiality, O.Ctrl_Channel, O.Mgmt_Path O.Trust_Backup
P.Default_Config	O.Trusted_Recovery
P.Information_Update	O.Patches, O.Validation
P.Integrity	O.Cfg_Integrity, O.Cfg_Manage, O.Ctrl_Channel, O.Mgmt_Path
P.Interoperability	O.Protocols
P.Notify	O.Alarm
P.Peer	O.Access_Control, O.Ctrl_Channel, O.Ctrl_I&A, O.Protect_Addresses
P.Procedures	O.Cfg_Confidentiality, O.Cfg_Manage, O.Mgmt_Path, O.Patches, O.Traf_Audit, O.Trust_Backup
P.Reliable_Transport	O.Ctrl_Channel, O.Priority_of_Service, O.Protocols, O.Replay_Prevent, O.Traf_Audit

Policy/Threat/Assumptions	Security Objectives
P.Survive	O.Alarm, O.Cfg_Manage, O.Fail_Secure, O.Lifecycle, O.Test, O.Trust_Backup, O.Trusted_Recovery, O.Validation
P.SysAssur	O.Lifecycle, O.Test, O.Validation
T.Analysis	O.Ctrl_Channel, O.Detect_Connection, O.Mgmt_Path, O.Protect_Addresses
T.Capture	O.Ctrl_Channel, O.Detect_Connection, O.Mgmt_Path
T.Compromised_Node	O.Priority_Of_Service, O.Protect_Addresses, O.Traf_Audit, O.Trusted_Recovery
T.Covert	O.Unused_Fields
T.Cryptanalytic	O.Ctrl_Channel, O.Mgmt_Path
T.Denial	O.Ctrl_Channel, O.Priority_Of_Service, O.Replay_Prevent, O.Traf_Audit
T.Fail	O.Alarm, O.Fail_Secure, O.Trust_Backup, O.Trusted_Recovery, O.Validation

Policy/Threat/Assumptions	Security Objectives
T.Flaw	O.Lifecycle, O.Patches, O.Test O.Validation
T.Hostile_Admin	O.Trust_Backup, O.Trusted_Recovery
T.Mgmt_Error	O.Cfg_Manage, O.Trust_Backup, O.Trusted_Recovery
T.Modify	O.Ctrl_Channel, O.Trusted_Recovery, O.Validation,
T.Ntwk_Map	O.Ctrl_Channel, O.Detect_Connection, O.Protect_Addresses, O.Mgmt_Path
T.Replay_Attack	O.Access_Control, O.Ctrl_Channel, O.Ctrl_I&A, O.Detect_Connection, O.Mgmt_I&A, O.Replay_Prevent
T.Spoof	O.Ctrl_I&A, O.Detect_Connection, O.Protect_Addresses
T.Unauth_Mgmt_Access	O.Access_Control, O.Detect_Connection, O.Trust_Backup, O.Trusted_Recovery

Security Objectives for the Environment	
Policy/Threat/Assumptions	**Environmental Security Objectives**
A.Audit_Review	OE.Admin_Audit, OE.Audit_Review
A.Cryptanalytic	OE.Cryptography
A.Environmental	OE.Environment
A.ExpAgent	OE.Admin_Audit OE.Attr_Mgt, OE.Audit_Review, OE.Cryptography, OE.Mgmt_I&A, OE.Personnel, OE.Physical,
A.Physical	OE.Environment, OE.Physical
A.Time_Source	OE.Admin_Audit, OE.Synchronization
A.Train	OE.Guide_Docs, OE.Personnel
P.Accountability	OE.Admin_Audit, OE.Guide_Docs OE.Mgmt_I&A
P.Audit_Admin	OE.Admin_Audit, OE.Audit_Review, OE.Mgmt_I&A
P.Authentication	OE.Admin_Audit, OE.Mgmt_I&A
P.Guidance	OE.Guide_Docs
P.Information_Update	OE.Guide_Docs
P.Procedures	OE.Admin_Audit, OE.Audit_Review, OE.Guide_Docs
P.SysAssur	OE.Guide_Docs
T.Compromised_Node	OE.Audit_Review

Policy/Threat/Assumptions	Environmental Security Objectives
T.Fail	OE.Environment, OE.Physical
T.Hostile_Admin	OE.Admin_Audit, OE.Audit_Review, OE.Mgmt_I&A, OE.Personnel
T.Mgmt_Error	OE.Admin_Audit, OE.Personnel
T.Modify	OE.Attr_Mgt, OE.Personnel
T.Ntwk_Map	OE.Physical
T.Replay_Attack	OE.Mgmt_I&A
T.Spoof	OE.Mgmt_I&A
T.Unauth_Mgmt_Access	OE.Admin_Audit, OE.Audit_Review OE.Mgmt_I&A, OE.Personnel, OE.Physical

Table 6-2 Tracing of Security Objectives to the TOE Security Environment

Security Objectives for the TOE	
Objectives	**Policy/Threat/Assumptions**
O.Access_Control	A.ExpAgent, P.Authentication, P.Availability, P.Peer, T.Replay_Attack, T.Unauth_Mgmt_Access
O.Alarm	P.Availability, P.Notify, P.Survive, T.Fail
O.Cfg_Confidentiality	P.Confidentiality, P.Procedures
O.Cfg_Integrity	P,Integrity

Objectives	Policy/Threat/Assumptions
O.Cfg_Manage	P.Integrity, P.Procedures, P.Survive, T.Mgmt_Error
O.Ctrl_Channel	A.ExpAgent, P.Confidentiality, P.Integrity, P.Peer, P.Reliable_Transport, T.Analysis, T.Capture, T.Cryptanalytic, T.Denial, T.Modify, T.Ntwk_Map, T.Replay_Attack
O.Ctrl_I&A	A.ExpAgent, P.Accountability, P.Authentication, P.Peer, T.Replay_Attack, T.Spoof
O.Detect_Connection	A.ExpAgent, T.Analysis, T.Capture, T.Ntwk_Map, T.Replay_Attack, T.Spoof, T.Unauth_Mgmt_Access
O.Fail_Secure	P.Availability, P.Survive, T.Fail, T.Trans_Error
O.Lifecycle	P.Accountability, P.Survive, P.SysAssur, T.Flaw

Objectives	Policy/Threat/Assumptions
O.Mgmt_Path	A.ExpAgent, P.Confidentiality, P.Integrity, P.Procedures, T.Analysis, T.Capture, T.Cryptanalytic, T.Ntwk_Map
O.Patches	P.Informaiton_Update, P.Procedures, T.Flaw
O.Priority_Of_Service	P.Reliable_Transport, T.Compromised_Node, T.Denial
O.Protect_Addresses	A.ExpAgent, P.Peer, T.Analysis, T.Compromised_Node, T.Ntwk_Map, T.Spoof
O.Protocols	P.Interoperability, P.Reliable_Transport
O.Replay_Prevent	A.ExpAgent, P.Availabiltiy, P.Reliable_Transport, T.Denial, T.Replay_Attack
O.Test	P.Survive, P.SysAssur, T.Flaw

Objectives	Policy/Threat/Assumptions
O.Traf_Audit	A.ExpAgent, A.Time_Source, P.Accountability, P.Procedures, P.Reliable_Transport, T.Compromised_Node, T.Denial
O.Trust_Backup	A.ExpAgent, P.Confidentiality, P.Procedures, P.Survive, T.Fail, T.Hostile_Admin, T.Mgmt_Error, T.Unauth_Mgmt_Access
O.Trusted_Recovery	P.Default_Config, P.Survive, T.Compromised_Node, T.Fail, T.Hostile_Admin, T.Mgmt_Error, T.Unauth_Mgmt_Access
O.Unused_Fields	A.ExpAgent, T.Covert
O.Validation	P.Information_Update, P.Survive, P.SysAssur, T.Fail, T.Flaw, T.Modify

Security Objectives for the Environment	
Environmental Objectives	**Policy/Threat/Assumptions**
OE.Admin_Audit	A.Audit_Review, A.ExpAgent, A.Time_Source, P.Accountability, P.Audit_Admin, P.Authentication, P.Procedures, T.Hostile_Admin, T.Mgmt_Error, T.Unauth_Mgmt_Access
OE.Attr_Mgt	A.ExpAgent, T.Modify
OE.Audit_Review	A.Audit_Review, A.ExpAgent, P.Audit_Admin, P.Procedures, T.Compromised_Node, T.Hostile_Admin, T.Unauth_Mgmt_Access
OE.Cryptography	A.Cryptanalytic, A.ExpAgent
OE.Environment	A.Environmental, A.Physical, T.Fail
OE.Guide_Docs	A.Train, P.Accountability, P.Guidance, P.Information_Update, P.Procedures, P.SysAssur
OE.Personnel	A.ExpAgent, A.Train, T.Hostile_Admin, T.Mgmt_Error, T.Modify, T.Unauth_Mgmt_Access

Environmental Objectives	Policy/Threat/Assumptions
OE.Physical	A.ExpAgent, A.Physical, T.Fail, T.Ntwk_Map, T.Unauth_Mgmt_Access
OE.Synchronization	A.Time_Source

6.1.1 Policies

P.Accountability: Individual accountability
Organizations that use the TOE for transmitting information, persons in network management roles and developers shall be held accountable for their actions.

Rationale:

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit supports P.Accountability by ensuring that those in network management roles can be held accountable for their actions within the network management system. The audit records will report, at a minimum, the identity of the network management person, the actions of the network management person within the system, time and date.

O.Ctrl_I&A: Control Identification and Authentication
O.Ctrl_I&A supports P.Accountability through the identification and authentication in accordance with the access control policy to ensure that organizations can be held accountable for their actions.

OE.Guide_Docs: Guidance Documentation
OE.Guide_Docs supports P.Accountability by holding developers accountable for providing guidance documentation

O.Lifecycle: Lifecycle Security
O.Lifecycle supports P.Accountability by holding developers accountable for the preservation or enhancement of security features when releasing upgrades to hardware, software or firmware.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A supports P.Accountability through the identification and authentication of management personnel to ensure that they can be held accountable for their actions.

O.Traf_Audit: Audit Traffic Records with Identity
O.Traf_Audit supports P.Accountability by ensuring that clients can be held accountable for their actions through the generation and analysis of traffic records. At a minimum, the traffic records will identify the nodes involved in data transfers, the size of the traffic that was transmitted, time and date. As an example, traffic audit records can hold organizations accountable when sending more traffic than allowed thus consuming more bandwidth resulting in the denial of service to other clients.

P.Audit_Admin: Audit Management Personnel Data Information
The network management system shall be able to generate and transmit audit records. Audit records shall be provided & include enough information to determine the Network Management Administrator or the Network Management Security Administrator and the date, time, and actions that occurred during the session. Audit records shall be reviewed on a periodic basis.

Rationale:

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit supports P.Audit_Admin by ensuring that those in a network management role can be held accountable for their actions within the network management system. The audit records will report, at a minimum, the identity of the network management person, the actions of the network management person within the system, time and date.

OE.Audit_Review: Review of Audit Records
OE.Audit_Review supports P.Audit_Admin by ensuring the periodic review of audit records.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A supports P.Audit_Admin by ensuring that those persons in network management roles are identified and authenticated by the system prior to session establishment.

P.Authentication: Authentication of Operators and Nodes
The TOE shall support authentication of Network Performance Management Operators, Network Management Administrators, and Network Management Security Administrators. The TOE shall support authentication of peer nodes.

O.Access_Control: Network Access Control
O.Access_Control supports P.Authentication in that authentication must occur in order for an access control policy to be effective.

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit supports P.Authentication in that in order to provide audit records the Network Management Administrator or Network Management Security Administrator must be authenticated before assuming their role.

O.Ctrl_I&A: Control Identification and Authentication
O.Ctrl_I&A directly supports P.Authentication by allowing connectivity only after identification and authentication.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A supports P.Authentication in that authentication must occur prior to assuming a role.

P.Availability: Network Availability
Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.

Rationale:

O.Access_Control: Network Access Control
O.Access_Control supports P.Availability by only allowing authorized use of the network. Access is blocked to all that are not authorized thus preventing an undue burden on the TOE and the network.

O.Alarm: Alarm Notification for Security Risks
O.Alarm supports P.Availability by ensuring that the network will be available to clients by detecting and alerting failures, errors or security related events. Alarms allow for a quick response to correct the problem and have the network properly operating and once again available to clients.

O.Fail_Secure: Preservation of Secure State for Failures
O.Fail_Secure supports P.Availability by ensuring the availability of the network by preserving the secure state of the system during downtime. Preservation of the system allows for a quick return to proper operating conditions without having to re-configure the system.

O.Priority_Of_Service: Provide Priority of Service
O.Priority_Of_Service supports P.Availabiltiy by ensuring that one client cannot consume more than their share of processing time and bandwidth, thus causing network resources to be unavailable to other clients.

O.Replay_Prevent: Prevent Replay Attacks
O.Replay_Prevent supports P.Availabilty by ensuring that old or duplicate packets are capable of being rejected so that network resources are not unduly utilized.

P.Confidentiality: Information Confidentiality
Statistical data, configuration and connectivity information will remain confidential, both in real-time and as stored data. To aid in retaining confidentiality, the TOE must be able to support a robust cryptographic infrastructure. The TOE must be capable of cryptography or support interfaces to cryptographic devices.

Rationale:

O.Cfg_Confidentiality: Network Configuration Confidentiality
O.Cfg_Confidentiality supports P.Confidentiality through the assurance that configuration and connection information remains confidential.

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel directly supports P.Confidentiality by ensuring the confidentiality of control information necessary for transmission.

O.Mgmt_Path: Trusted Path for Management Data
O.Mgmt_Path directly supports P.Confidentiality by ensuring the confidentiality of network management data.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
O.Trust_Backup directly supports P.Confidentiality by ensuring the confidentiality of stored network files and configuration parameters.

P.Default_Config: Default Configuration
The default configuration settings for the TOE will have all functions that weaken or break TOE security functions disabled. All functions contributing to TOE Security Functions shall be enabled by default.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery supports P.Default_Config by ensuring the recovery to a secure state after a failure. If the recovery is to revert to the default settings then security of the network will be maintained.

P.Guidance: Installation and Usage Guidance
Guidance documents will be provided for the secure installation, configuration and maintenance of the switches and routers.

Rationale:

OE.Guide_Docs: Guidance Documentation
OE.Guide_Docs ensures that documentation will be provided to provide guidance for proper installation, configuration and maintenance of the TOE.

P.Information_Update: TOE Informational Updates
Ensure the integrity of TOE informational documents, known anomalies, patches, upgrades, etc. upon receipt. These documents, patches, upgrades, etc. will be released and distributed on a scheduled timely basis.

Rationale:

OE.Guide_Docs: Guidance Documentation
OE.Guide_Docs supports P.Information_Update through the assurance that guidance documentation will be provided on a timely basis.

O.Patches: Security Fixes and Patches
O.Patches directly supports P.Information_Update by ensuring that the latest patches have been distributed and are installed in the network.

O.Validation: Validation of HW/SW/FW
O.Validation directly supports P.Information_Update by ensuring the integrity of all HW/SW/FW patches and upgrades.

P.Integrity: Content Integrity
Management and control information shall retain its content integrity during transmission. All information shall retain its integrity as stored information.

Rationale:

O.Cfg_Integrity: Configuration Integrity
O.Cfg_Integrity supports P.Integrity by ensuring that stored information pertaining to the TOE retains content integrity.

O.Cfg_Manage: Manage Configuration Data
O.Cfg_Manage supports P.Integrity by ensuring the integrity of network management information as stored information.

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel supports P.Integrity by ensuring that control information retains its integrity as it is transferred among peer TOEs.

O.Mgmt_Path: Trusted Path for Management Data
O.Mgmt_Path supports P.Integrity by ensuring that network management information retains its integrity as it is transferred between the TOE and the network management station.

P.Interoperability: Interoperability
The TOE shall be interoperable with switches/routers of other vendors. Standardized, nonproprietary, protocols (routing, signalling, etc.) shall be implemented in the TOE. The vendor may choose to implement some proprietary protocols however, for interoperability the vendor shall also implement standardized protocols in the TOE.

O.Protocols: Protocols
O.Protocols supports P.Interoperability by ensuring that protocols are implemented in the TOE for interoperability.

P.Notify: Notification of Failure
The TOE and the TSE will be capable of alerting and providing alarms, e.g. via SNMP3 traps, in the event of a component, firmware, hardware or software failure.

Rationale:

O.Alarm: Alarm Notification for Security Risks
O.Alarm supports P.Notify by ensuring that the TOE will be capable of detecting and alerting of a failure or error with any component.

P.Peer: Peer Nodes
Secure nodes will have the ability to accept traffic from trusted and untrusted nodes. Traffic will be filtered between trusted & untrusted nodes to protect information.

Rationale:

O.Access_Control: Network Access Control
O.Access_Control supports P.Peer by ensuring that only those who are authorized can gain access to the secure node.

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel supports P.Peer by ensuring the integrity and confidentiality of all control data transferred between peer TOEs.

O.Ctrl_I&A: Control Identification & Authentication
O.Ctrl_I&A support P.Peer in conjunction with O.Access_Control. O.Ctrl_I&A ensures that connectivity will be provided only upon the request of authorized entities that have been properly identified and authenticated in accordance with the access control policy.

O.Protect_Addresses: Protect Addresses
O.Protect_Addresses ensures that traffic will be transmitted between trusted and untrusted TOEs by providing confidentiality and integrity of the transmitting and receiving authorized entities' addresses.

P.Procedures: Procedures for Management of Information
Procedures will be in place to restrict the inadvertent disclosure or modification of sensitive information or improper utilization of resources in the TSE. Examples of sensitive information include, but are not limited to, printed material detailing operations procedures, equipment installation procedures, audit files, configuration files, network diagrams, information across physical connections and network test results.

Rationale:

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit supports P.Procedures by ensuring that procedures are in place for storing and protecting audit records of network management personnel.

OE.Audit_Review: Review of Audit Records
OE.Audit_Review supports P.Procedures by ensuirng that audit records are periodically reviewed. Review of audit records can uncover improper utilization of resources.

O.Cfg_Confidentiality: Network Configuration Confidentiality
O.Cfg_Confidentiality supports P.Procedures by ensuring that procedures are in place to retain the confidentiality of configuration and connectivity information.

O.Cfg_Manage: Manage Configuration Data
O.Cfg_Manage supports P.Procedures by ensuring that procedures are in place to capture and retain configuration and connection information and to assure storage integrity.

OE.Guide_Docs: Guidance Documentation
OE.Guide_Docs supports P.Procedures by ensuring detailed procedures for the proper installation, maintenance, configuration and utilization of the TOE and TOE security functions are provided.

O.Mgmt_Path: Trusted Path for Management Data
O.Mgmt_Path supports P.Procedures by ensuring the integrity and confidentiality of all management data transferred between the TOE and the network management station.

O.Patches: Security Fixes and Patches
O.Patches supports P.Procedures by ensuring that procedures are in place for the notification of, distribution and installation of the latest patches and security to ensure the proper operation and utilization of network resources. Software that is functioning properly and free of flaws will minimize the risk of the inadvertent disclosure of information.

O.Traf_Audit: Audit Traffic Records with Identity
O.Traf_Audit supports P.Procedures by ensuring that procedures are in place to generate and maintain the integrity of traffic audit records.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
O.Trust_Backup supports P.Procedures by ensuring that procedures are in place to maintain the consistency and proper storage of replicated network information for avoidance of disclosure or modification of the files.

P.Reliable_Transport: Reliable_Transport
Protocols specifying reliable transport and error detection mechanisms shall be implemented for network management and control.

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel supports P.Reliable_Transport by ensuring that integrity of control data is able to be verified upon receipt.

O.Priority_of_Service: Provide Priority of Service
O.Priority_of_Service supports P.Reliable_Transport by ensuring reliable transport of information as dictated by the applied priority of service.

O.Protocols: Protocols
O.Protocols directly supports P.Reliable_Transport by ensuring that standardized protocols are implemented in the TOE for the reliable transport of traffic.

O.Replay_Prevent: Prevent Replay Attacks
O.Replay_Prevent supports P.Reliable_Transport by ensuring that old and duplicate packets are able to be detected and rejected so that they do not interfere with other communications.

O.Traf_Audit: Audit Traffic Records with Identity
O.Traf_Audit supports P.Reliable_Transport by ensuring the reliability of traffic communications through the capture and analysis of network traffic statistics.

P.Survive: Network Survivability & Recovery
Resources shall be able to recover from hostile attempts against security. Resources must also be able to recover from errors that may occur during transmission. The network must be able to be resistant, or recover in a reasonable amount of time from a hardware or software failure. Any circumstances that could result in a partial recovery shall be documented.

Rationale:

O.Alarm: Alarm Notification for Security Risks
O.Alarm supports P.Survive by ensuring the survivability of the TOE and the TSF by providing notification of security related events, failures or errors, which allow for a quick response to correct the problem and restore the TOE and TSF to normal operating conditions.

O.Cfg_Manage: Manage Configuration Data
O.Cfg_Manage supports P.Survive through the retention of configuration and connection information as well as storage integrity of this information. In this manner, any necessary network configuration can be quickly re-created thus assisting in promoting survivability.

O.Fail_Secure: Preservation of Secure State for Failures
O.Fail_Secure supports P.Survive by offering resiliency and survivability through the preservation of the secure state of the system in the event of a component or power failure.

O.Lifecycle: Lifecycle Security
O.Lifecycle supports P.Survive by ensuring that security functions are preserved throughout the life of the TOE so that resources can retain the ability to recover from or be resistant to errors or attempts against security.

O.Test: Testing of the TOE and TSF
O.Test supports P.Survive by ensuring that the network will be able to survive or recover from a failure.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
O.Trust_Backup supports P.Survive through the replication of all TOE and network files, including configuration parameters that will ensure a quick recovery in the event of a hostile attempt or a failure in operations with the TOE or the primary management system.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery supports P.Survive with the assurance that the TOE is able to recover to a secure state after a failure.

O.Validation: Validation of HW/SW/FW
O.Validation supports P.Survive by ensuring that all hardware, software and firmware is correctly installed and functioning properly which provides assurance that the network will be able to resist, recover or survive a failure, error or an attempt against security.

P.SysAssur: Hardware, Software, and Firmware Security Integrity
Features and procedures to validate the integrity and the expected performance of the initial and all upgraded versions of hardware, software and firmware shall be provided. Integrity shall be ensured at the time of initial installation and at the time of software upgrades and firmware swap-outs as well.

Rationale:

OE.Guide_Docs: Guidance Documentation
OE.Guide_Docs supports P.SysAssur by ensuring that TOE and TSF features, procedures and expected performance are explained.

O.Lifecycle: Lifecycle Security
O.Lifecycle supports P.SysAssur by ensuring that through features and procedures the integrity and proper performance of the TOE and TSF is maintained.

O.Test: Testing of the TOE and TSF
O.Test supports P.SysAssur by ensuring the proper functioning and performance of the TOE and TSF

O.Validation: Validation of HW/SW/FW
O.Validation directly supports P.SysAssur by ensuring, through features and procedures, the integrity and proper performance of all hardware, software and firmware.

6.1.2 Threats

T.Analysis: Traffic Analysis
An attacker collects source and destination addresses, volume of data and time of day that messages are sent.

Rationale:

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel mitigates the threat of T.Analysis by retaining the confidentiality of control and signalling information and supporting a cryptographic infrastructure.

O.Detect_Connection: Detection of Unauthorized Connections
O.Detect_Connection counters T.Analysis through the ability of the TOE to detect and alert of unauthorized connections.

O.Mgmt_Path: Trusted Path for Management Data
O.Mgmt_Path counters T.Analysis by ensuring integrity and confidentiality of all management data.

O.Protect_Addresses: Protect Addresses
O.Protect_Addresses counters T.Analysis by protecting the confidentiality and integrity of source and recipient authorized addresses thus preventing attackers from discovering true addresses.

T.Capture: Unauthorized Network Access to Capture Data
An attacker eavesdrops, taps into the transmission line, or otherwise captures data being transferred on a communications channel.

Rationale:

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel counters T.Capture by ensuring the confidentiality and integrity retention of control plane information

O.Detect_Connection: Detection of Unauthorized Connections
O.Detect_Connection counters the threat of T.Capture through the ability to detect any unauthorized connections.

O.Mgmt_Path: Trusted Path for Management Data
O.Mgmt_Path counters T.Capture by providing a trusted path for management

data communication which hinders an attackers attempt to capture network management data.

T.Compromised_Node: Compromised Node
A node becomes compromised, altering TOE configuration files and/or the routing table, causing incorrect operations of the TOE, disabling of TOE security features, and/or re-routing of traffic which could be re-routed through an unauthorized node.

Rationale:

OE.Audit_Review: Review of Audit Records
OE.Audit_Review counters T.Compromised_Node through the review and analysis of traffic audit records, which can uncover unusual network traffic patterns.

O.Priority_Of_Service: Provide Priority of Service
O.Priority_Of_Service counters T.Compromised_Node through the control and enforcement of the priority of service policy that hinders an attempt to manipulate a node to only transmit traffic of a specified priority.

O.Protect_Addresses: Protect Addresses
O.Protect_Addresses counters the threat T.Compromised_Node by ensuring the confidentiality and integrity of addresses.

O.Traf_Audit: Audit Traffic Records with Identity
O.Traf_Audit, in conjunction with OE.Audit_Review, counters T.Compromised_Node with the ability to capture continuous unusual activity through the generation of traffic records.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery mitigates T.Compromised_Node by ensuring the recovery of the TOE to a secure state, without security compromise, after a disruption or discontinuity of operations.

T.Covert: Covert Channels
Covert Channels are used to hide information in any unused fields in order to send information without being monitored.

Rationale:

O.Unused_Fields: Unused Fields
O.Unused_Fields directly counters T.Covert in that any unused fields are blocked or properly set so that they cannot be used to hide and transmit information.

T.Cryptanalytic: Cryptoanalysis for Theft of Information
An attacker attempts cryptoanalysis on encrypted data in order to recover message content.

Rationale:

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel counters the threat of T.Cryptanalytic by ensuring the confidentiality of control and signalling information through the support of a cryptographic infrastructure and through the retention of control information integrity.

O.Mgmt_Path: Trusted Path for Management Data
O.Mgmt_Path counters T.Cryptanalytic by ensuring the confidentiality of management data through the support of a cryptographic infrastructure and through the retention of management data integrity.

T.Denial: Denial of Service
An attacker executes commands, sends more than allowed high priority traffic, or performs other operations that cause undue burden on the network therefore making system resources unavailable to authorized clients, e.g., resulting in service denial.

Rationale:

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel counters the threat T.Denial by ensuring the integrity of control information, which can be manipulated and cause resources to become unavailable to other clients.

O.Priority_Of_Service: Provide Priority of Service
O.Priority_Of_Service, counters T.Denial by controlling and enforcing a subscribed priority of service which ensures one priority of traffic will not unduly interfere with or delay traffic of differing priorities of service.

O.Replay_Prevent: Prevent Replay Attacks
O.Replay_Prevent counters T.Denial by blocking replayed messages that consume network resources. Therefore, the ability of the TOE to block replayed messages will help ensure that network resources are available to authorized clients.

O.Traf_Audit: Audit Traffic Records with Identity
O.Traf_Audit mitigates the threat of T.Denial through the capture of traffic statistics that assist in identifying the TOE responsible for the monopolization of

network resources.

T.Fail: Component or Power Failure
Failure of one or more system components or a power failure results in the loss of system-critical functionality and system data.

Rationale:

O.Alarm: Alarm Notification for Security Risks
O.Alarm mitigates the threat T.Fail by allowing for a quick response to correct the error or failure.

OE.Environment: Environmental Protection
OE.Environment mitigates the threat of T.Fail by having the TOE developed so that it is able to protect itself against environmental threats such as fire, power outages, etc.

O.Fail_Secure: Preservation of Secure State for Failures
O.Fail_Secure helps to counter the threat T.Fail by ensuring that the TOE and the TSF can return to a secure state.

OE.Physical: Physical Protection
OE.Physical mitigates T.Fail through the physical protection of resources which helps to prevent a malicious or unintentional, yet harmful physical attack.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
O.Trust_Backup mitigates the threat T.Fail through the assurance of a replicated version of network data that will be able to quickly return the TOE and TSF to proper operation.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery mitigates the threat T.Fail by ensuring that the TOE will recover to a secure state, without security compromise, after a discontinuity of operations. O.Trusted_Recovery also ensures that replaced failed components, when re-integrated into the system, will recover such that it will not cause errors or security breaches in other parts of the network.

O.Validation: Validation of HW/SW/FW
O.Validation counters the threat T.Fail by ensuring that all components are correctly installed and properly functioning.

T.Flaw: Flaws in hardware, software or firmware
Flaws in hardware, software or firmware cause vulnerabilities in the TOE and the TSF.

O.Lifecycle: Lifecycle Security
O.Lifecycle mitigates the threat of T.Flaw by preserving the proper operation of TOE security functions throughout the operational lifetime of the TOE.

O.Patches: Security Fixes and Patches
O.Patches mitigates the threat of T.Flaw by ensuring that the most recent fixes and patches are installed, which will ensure against flaws causing vulnerabilities in the TOE and TSF.

O.Test: Testing of the TOE and TSF
O.Test mitigates the threat of T.Flaw by discovering flaws that may hinder the operation or cause security vulnerabilities of the TOE and TSF.

O.Validation: Validation of HW/SW/FW
O.Validation mitigates the threat of T.Flaw by validating the integrity, proper installation and functioning of all hardware, software and firmware, which can assist in identifying flaws that may cause vulnerabilities in the TOE and the TSF.

T.Hostile_Admin: Management Personnel Abuse of Network Authorization
A Network Management Administrator or Network Management Security Administrator intentionally abuses granted authorizations to inappropriately access or modify information, e.g. configuration data, audit data, password files, or other mishandling of sensitive data files.

Rationale:

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit counters the threat of T.Hostile_Admin since the threat of privileges being abused are reduced if it is known that actions and identities are monitored and recorded.

OE.Audit_Review: Review of Audit Records
OE.Audit_Review mitigates the threat of T.Hostile_Admin by making it known that actions are monitored and reviewed on a periodic basis.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A mitigates the threat of T.Hostile_Admin by making it known that the identity of network management personnel is captured in audit records.

OE.Personnel: Trustworthy Personnel
OE.Personnel counters the threat of T.Hostile_Admin through the hiring and

retention of trustworthy and competent personnel.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
O.Trust_Backup mitigates the threat of T.Hostile_Admin by ensuring a replication of network files. If the primary system is caused to fail then the replicated system can be quickly put into operation to ensure a continuity of operation. Or, if network files are not stored on a secondary management station but on another storage device then network parameters are still preserved.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery mitigates the threat of T.Hostile_Admin by ensuring that the network is able to recover to a secure state, without security compromise, after a discontinuity of operations.

T.Mgmt_Error: Management Error
A person in a network management role makes a security relevant error that results in inappropriate access or modification of information, or inappropriate utilization of resources.

Rationale:

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit mitigates the threat of T.Mgmt_Error by being able to identify the error so that the action and its effects can be corrected.

O.Cfg_Manage: Manage Configuration Data
O.Cfg_Manage mitigates T.Mgmt_Error through the capture and retention of configuration and connection information, which will allow for the recovery of TOE and network information.

OE.Personnel: Trustworthy Personnel
OE.Personnel counters T.Mgmt_Error by hiring and maintaining competent and trustworthy personnel.

O.Trust_Backup: Integrity of System Data Replication
O.Trust_Backup mitigates the threat of T.Mgmt_Error by being able to continue operations from the second system while restoring the primary system, in the event that the error was severe.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery mitigates the threat of T.Mgmt_Error by ensuring the recovery to a secure state, without security compromise, after a discontinuity of operations.

T.Modify: Modification of Protocols
An attacker makes unauthorized modifications, or manipulates protocols (e.g. routing, signalling, etc.) en-route.

Rationale:

OE.Attr_Mgt: Manage Attributes
OE.Attr_Mgt mitigates the threat T.Modify. Network Management Administrators and Network Management Security Administrators have privileges such that a hostile network management person could easily make modifications. However, this threat is mitigated when it is known that the identification of network management persons is captured and audited.

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel counters the threat T.Modify by ensuring that control and signalling information remains confidential and retains its integrity.

OE.Personnel: Trustworthy Personnel
OE.Personnel counters the threat of T.Modify by hiring trustworthy employees who can be trusted not to abuse their privilege and make unauthorized modifications or manipulate the configurations or protocols in use.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery mitigates the threat of T.Modify by ensuring that in the event that T.Modify cause a discontinuity in operation, the TOE and the network will be able to recover to a secure state.

O.Validation: Validation of HW/SW/FW
O.Validation counters the threat of T.Modify by validating the integrity and proper operation of all hardware, software and firmware prior to being implemented in the operational TOE or the network.

T.Ntwk_Map: Network Mapping
An attacker attempts to map the network - thus obtaining addresses of nodes, routing table information and physical locations.

Rationale:

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel counters the threat of T.Ntwk_Map by ensuring the confidentiality and integrity of control and signalling information.

O.Detect_Connection: Detection of Unauthorized Connections
O.Detect_Connection counters the threat of T.Ntwk_Map through the detection

of unauthorized connections.

OE.Physical: Physical Protection
OE.Physical counters T.Ntwk_Map by ensuring the physical protection of TOE resources thus eliminating the threat of an attacker making an unauthorized connection in an attempt to capture network information.

O.Protect_Addresses: Protect Addresses
O.Protect_Addresses counters T.Ntwk_Map by ensuring the confidentiality and integrity of the transmitting and receiving addresses.

O.Mgmt_Path: Trusted path for Management Data
O.Mgmt_Path counters T.Ntwk_Map through the assurance of a trusted path for all management data. This trusted path protects the data and assists in increasing the difficulty for an attacker to obtain management data for analysis and discovery of network information.

T.Replay_Attack: Replay Attack
An attacker records a communication session in order to masquerade as an authenticated client to gain access to the TOE by playing back the previously recorded message. Management information could also be recorded and re-played in an attempt to masquerade as an authenticated Network Management Administrator or a Network Management Security Administrator to gain access to network management resources.

Rationale:

O.Access_Control: Access Control Policy
O.Access_Control mitigates the threat of T.Replay_Attack through the implementation of an access control policy, which increases the difficulty for an attacker to gain access to the TOE and the network.

O.Ctrl_Channel: Trusted Channel for Control Data
O.Ctrl_Channel counters the threat of T.Replay_Attack by ensuring the confidentiality and integrity of control and signalling information with the support of a cryptographic infrastructure.

O.Ctrl_I&A: Control Identification and Authentication
O.Ctrl_I&A mitigates the threat of T.Replay_Attack by requiring identification and authentication which increases the difficulty for an attacker to gain access to the TOE.

O.Detect_Connection: Detection of Unauthorized Connections
O.Detect_Connection counters the threat of T.Replay_Attack by ensuring the

detection of unauthorized connections thus eliminating the ability to record and therefore replay messages in an attempt to gain access to the TOE and network resources.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A mitigates the threat of T.Replay_Attack by requiring identification and authentication which increases the difficulty for an attacker to gain access to network management resources.

O.Replay_Prevent: Prevent Replay Attacks
O.Replay_Prevent directly counters the threat of T.Replay_Attack. O.Replay_Prevent ensures that the TOE is capable of rejecting old or duplicate packets in order to protect itself against a replay attack.

T.Spoof: Spoofing Attack
A client masquerades as an authorized person by obtaining a network address in an attempt to gain access to TOE resources. An unauthorized node may attempt to access a network by using a valid network address.

Rationale:

O.Ctrl_I&A: Control Identification and Authentication
O.Ctrl_I&A counters T.Spoof by enforcing identification and authentication which increases the difficulty for an attacker to gain access to the TOE, thus increasing the difficulty for trying to execute a spoofing attack.

O.Detect_Connection: Detection of Unauthorized Connections
O.Detect_Connection counters T.Spoof by ensuring the detection of unauthorized connections, which then hinders the ability of an attacker to capture network addresses.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A counters T.Spoof by enforcing identification and authentication which increases the difficulty for an attacker to gain access to the TOE, thus increasing the difficulty for trying to execute a spoofing attack.

O.Protect_Addresses: Protect Addresses
O.Protect_Addresses counters T.Spoof by ensuring the confidentiality and integrity of the transmitting and receiving addresses which inhibits an attackers' ability to obtain legitimate network addresses.

T.Unauth_Mgmt_Access: Unauthorized Access to the Management port
An attacker may access, or a person in a network management role may abuse their privileges and gain access to the management port, either through Telnet, RMON etc., to re-configure the network, cause denial of service to clients, monitor traffic to perform traffic analysis, etc.

Rationale:

O.Access_Control: Network Access Control
O.Access_Control counters the threat of T.Unauth_Mgmt_Access by limiting privileges through the implementation of an access control policy.

OE.Admin_Audit: Audit Records with Identity
OE.Admin_Audit mitigates the threat of abuses of privileges, T.Unauth_Mgmt_Access, through the audit of the actions of network management personnel with accountability.

OE.Audit_Review: Review of Audit Records
OE.Audit_Review mitigates the threat of T.Unauth_Mgmt_Access by making it known that actions are audited and reviewed on a periodic basis.

O.Detect_Connection: Detection of Unauthorized Connections
O.Dectect_Connection counters T.Unauth_Mgmt_Access by ensuring the detection of unauthorized connections, which assists in discovering unauthorized access to the management data.

OE.Mgmt_I&A: Management Identification and Authentication
OE.Mgmt_I&A mitigates the threat of T.Unauth_Mgmt_Access by identifying the network management person who will be audited and linked to their actions.

OE.Personnel: Trustworthy Personnel
OE.Personnel mitigates the threat of an abuse of privilege, T.Unauth_Mgmt_Access through the hiring and retention of trustworthy network management personnel on staff.

OE.Physical: Physical Protection
OE.Physical counters T.Unauth_Mgmt_Access by ensuring that resources are physically protected to prevent malicious attacks and unauthorized modification.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
O.Trust_Backup mitigates the threat of T.Unauth_Mgmt_Access by ensuring the storage and integrity of data files for the TOE. O.Trust_Backup allows for a

quick recovery in the event that unauthorized access to management data has occurred and the network parameters have been manipulated.

O.Trusted_Recovery: Trusted Recovery
O.Trusted_Recovery mitigates the threat of T.Unauth_Mgmt_Access by ensuring that the TOE is able to return to a secure state after a discontinuity in operation.

6.2 SECURITY REQUIREMENTS RATIONALE

This section presents tables that prove comprehensive coverage of security objectives. First, Table 6-2 is presented and shows that each objective covered by requirements. Following Table 6-2 are individual arguments for each objective coverage.

6.2.1 Functional Security Requirements Rationale

Table 6-3 Functional Component to Security Objective Mapping

Objectives	Requirements
O.Access_Control	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_UAU.2, FIA_UID.2, FTA_TSE.1
OE.Admin_Audit	FAU_GEN.1, FAU_GEN.2, FAU_SEL.1, FMT_MSA.1, FMT_MSA.3 FMT_MTD.1 FPT_STM.1, FPT_TDC.1
O.Alarm	FPT_AMT.1, FPT_TST.1
OE.Attr_Mgt	FAU_SAR.1, FMT_MSA.1, FMT_MTD.1, FMT_SMR.2
OE.Audit_Review	FAU_SAR.1, FPT_TDC.1

Objectives	Requirements
O.Cfg_Confidentiality	FTP_ITC.1, FTP_TRP.1
O.Cfg_Integrity	FPT_ITI.1, FPT_TST.1, FTP_ITC.1, FTP_TRP.1
O.Cfg_Manage	FTP_TRP.1
OE.Cryptography	FTP_ITC.1 FTP_TRP.1
O.Ctrl_Channel	FDP_IFF.1, FDP_UIT.1, FTP_ITC.1, FPT_ITC.1, FPT_ITI.1
O.Ctrl_I&A	FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_UAU.2, FIA_UID.2, FTA_TSE.1
O.Detect_Connection	FPT_ITI.1, FPT_RPL.1
OE.Environment	FPT_FLS.1, FPT_RCV.3, FPT-RCV.4, FRU_FLT.1
O.Fail_Secure	FPT_FLS.1, FPT_RCV.3, FPT_RCV.4, FRU_FLT.1
OE.Guide_Docs	ADV_FSP.2, ADV_SPM.1, ALC_FLR.3, ALC_DVS.1, AGD_ADM.1, AGD_USR.1, AMA_EVD.1, AVA_MSU.1, AVA_VLA.1

Objectives	Requirements
O.Lifecycle	FPT_AMT.1, FPT_TDC.1, FPT_TST.1
O.Mgmt_Path	FDP_IFF.1, FDP_ITC.2, FDP_ETC.2, FDP_UIT.1, FPT_ITI.1, FTP_TRP.1
O.Patches	ALC_FLR.3, FMT_MOF.1
OE.Personnel	AGD_ADM.1, AGD_USR.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3
OE.Physical	FPT_PHP.1
O.Priority_Of_Service	FDP_IFF.1, FRU_PRS.2, FRU_FLT.1
O.Protect_Addresses	FDP_ITC.2, FDP_ETC.2, FPT_ITC.1, FTP_ITC.1, FTP_TRP.1
O.Protocols	FDP_ETC.2, FDP_ITC.2, FDP_UIT.1, FPT_FLS.1, FPT_ITI.1
O.Replay_Prevent	FDP_ETC.2, FDP_ITC.2 FDP_UIT.2, FPT_ITI.1, FPT_RPL.1
OE.Synchronization	FMT_MOF.1, FPT_STM.1

Objectives	Requirements
O.Test	AMA_SIA.2, ATE_COV.2, ATE_FUN.1, ATE_IND.2, AVA_SOF.1, AVA_VLA.1 FPT_AMT.1, FPT_TST.1
O.Traf_Audit	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SEL.1, FDP_IFF.1 FPT_STM.1, FPT_TDC.1
O.Trust_Backup	FDP_UIT.2
O.Trusted_Recovery	FPT_RCV.3, FPT_RCV.4, FPT_FLS.1
O.Unused_Fields	FPT_ITI.1
O.Validation	FPT_AMT.1, FPT_TST.1

O.Access_Control: Network Access Control
Implement an access control policy. The access control policy will be based on, but not limited to the following, the TOE's role (handling trusted only, untrusted or a mix of traffic), the TOE's identity (owned by an organization, owned by the network provider and supporting many organizations/clients), source and destination addresses, filtering at the port level (Telnet, SNMP,etc.), etc.

O.Access_Control is implemented in the TOE by FDP_ACC.1: Subset access control, and FDP_ACF.1: Security Attribute Based Access Control, which enforces the access control policy between TOE's wishing to communicate. FIA_UAU.2: User Authentication Before any Action and FIA_UID.2: User Identification, require identification and authentication in conjunction with the access control policy. O.Access_Control is also provided by FTA_TSE.1: TOE Session Establishment, which can deny session establishment to the TOE, and FDP_IFF.1: Simple Security Attributes and FDP_IFC.1: Subset Information Flow

Control, which require the information flow control policy to function in conjunction with the access control policy for receiving messages.

OE.Admin_Audit: Audit Records with Identity
The actions of Network Management Administrators and Network Management Security Administrators shall be audited. Audit records will be stored and maintained in accordance with the security policy.

OE.Admin_Audit is implemented by several requirements. In the TOE's environment by FPT_TDC.1: Inter-TSF Basic TSF Data Consistency, which ensures that audit records can be interpreted. FMT_MTD.1: Management of TSF Data, FAU_SEL.1: Selective Audit, FMT_MSA.1: Management of Security Attributes, and FMT_MSA.3: Static Attribute Initialization, give Network Management Security Administrators the privilege to be able to customize the audit logs. FAU_GEN.1 and FAU_GEN.2 directly implement this objective by generating audit logs and associating audit data with the responsible network management person. One important aspect of generating audit logs is capturing the time of the action, therefore FPT_STM.1: Reliable Time Stamps is an applicable requirement in support of OE.Admin_Audit.

O.Alarm: Alarm Notification for Security Risks
The TOE will be capable of detecting a failure or error with any component, hardware, software, or firmware. The TOE will provide alarming capabilities for notification of security related events and of a failure or error.

O.Alarm is implemented in the TOE by FPT_AMT.1: Abstract Machine Testing, and FPT_TST.1: TSF Testing, which require that tests are run to detect errors with the TSF.

OE.Attr_Mgt: Manage Attributes
The Network Management Security Administrator will manage the access control policy within the network management system to only give authorized network management persons the necessary functional abilities. Management personnel will be able to assume their privileged roles within the network management system only upon proper identification and authentication.

OE.Attr_Mgt is implemented by FAU_SAR.1: Audit Review, which gives Network Management Security Administrators the privilege to review all the audit records. FMT_MSA.1: Management of Security Attributes, FMT_MTD.1: Management of TSF Data, and FMT_SMR.2: Restrictions on Security Roles, implement OE.Attr_Mgt by restricting certain privileges of the network management system to different roles.

OE.Audit_Review: Review of Audit Records
All Audit records will periodically be reviewed. Network Performance Management operators will periodically review Network Traffic audit records.

OE.Audit_Review is implemented by FTP_TDC.1: Inter-TSF Basic TSF Data Consistency, which ensures that audit records can be interpreted. FAU_SAR.1: Audit Review implements OE.Audit_Review by requiring the review of audit records.

O.Cfg_Confidentiality: Network Configuration Confidentiality
Configuration and connectivity information will not be disclosed.

O.Cfg_Confidentiality is implemented by FPT_ITC.1: Inter-TSF Confidentiality during Transmission, and FTP_TRP.1: Trusted Path, which requires a trusted channel for control information that will protect such information from disclosure and a trusted path for management information.

O.Cfg_Integrity: Configuration Integrity
Audit files, configuration, connectivity information, and other information pertaining to the TOE will retain its content integrity. The TOE does not have to be responsible for storing this information.

O.Cfg_Integrity is implemented in the TOE by FPT_ITI.1: Inter-TSF Detection of Modification, and by FPT_TST.1: TSF Testing and FTP_TRP.1: Trusted Path and FTP_ITC.1: Inter-TSF Trusted Channel, which requires that TSF data is protected from modification during transmission, the detection of modifications, and the verification of the integrity of TSF data.

O.Cfg_Manage: Manage Configuration Data
Implement a plan in which to capture and retain configuration and connection information for each switch and/or router. The plan must assure storage integrity, identification of system connectivity and identification of system components.

O.Cfg_Manage is implemented in the TOE by FTP_TRP.1: Trusted Path, by providing a trusted path to transfer configuration and connectivity data from the TOE.

OE.Cryptography: Support of Cryptographic Infrastructure
The TOE must be able to support a cryptographic infrastructure in order to aid in providing confidentiality. The cryptographic infrastructure will support services including client registration, key management and segregation of communities of interest.

OE.Cryptography is implemented by FTP_ITC.1: Inter-TSF Trusted Channel, and FTP_TRP.1: Trusted Path which allow for the option to protect data from disclosure.

O.Ctrl_Channel: Trusted Channel for Control Data
Provide integrity and confidentiality of all control data transferred between peer TOEs. Provide a trusted channel that is distinct from and cannot be confused with other communications. To aid in providing confidentiality, the TOE must be able to support a cryptographic infrastructure. The cryptographic infrastructure will support services such as, client registration, key management and segregation of communities of interest.

O.Ctrl_Channel is implemented through the implementation of a trusted channel, FTP_ITC.1: Inter-TSF Trusted Channel, FDP_UIT.1: Data Exchange Integrity, FPT_ITC.1: Inter-TSF Confidentiality, and FPT_ITI.1: Inter-TSF Detection of Modification during Transmission, to protect against the disclosure and modification of information. O.Ctrl_Channel is also implemented through FDP_IFF.1: Simple Security Attributes, which requires a trusted channel for information flows.

O.Ctrl_I&A: Control Identification and Authentication
Connectivity will be provided between peer TOEs only upon the identification, authentication and authorization of the requesting and destination addresses in accordance with the access control policy.

O.Ctrl_I&A is implemented in the TOE by FDP_ACC.1: Subset Access Control, FDP_IFF.1: Simple Security Attributes and FDP_ACF.1: Security Attribute Based Access Control, for the enforcement of the access control policy, identification and authentication. O.Ctrl_I&A is also implemented by FTA_TSE.1: TOE Session Establishment, FDP_IFC.1: Subset Information Flow Control, FIA_UAU.2: User Authentication Before any Action, and FIA_UID.2: User Identification, which requires identification and authorization in order to establish a communications session and determine if information is from a trusted source.

O.Detect_Connection: Detection of Unauthorized Connections
The TOE will be able to detect and alert of unauthorized connections.

O.Detect_Connection is implemented in the TOE by: FPT_ITI.1: Inter-TSF

Detection of Modification, and FPT_RPL.1: Replay Detection. These requirements call for scanning ports, which will aid in the discovery of unauthorized connections.

OE.Environment: Environmental Protection
Resources shall be developed to provide protection against environmental threats, e.g., fire, earthquake, loss of power, etc.

OE.Environment is implemented by FTP_FLS.1: Failure with Preservation of Secure State, FPT_RCV.3: Automated Recovery without Undue Loss, and FPT_RCV.4: Function Recovery which will ensure a successful switch-over to the back-up power supply or preserve a secure state during a short power interruption. FRU_FLT.1: Degraded Fault Tolerance implements OE.Environment by ensuring TOE operation during natural disasters or power interruption.

O.Fail_Secure: Preservation of Secure State for Failures
Preserve the secure state of the system in the event of a component or power failure.

O.Fail_Secure is implemented in the TOE by FPT_FLS.1: Failure with Preservation of Secure State, FPT_RCV.3: Automated Recovery without Undue Loss, FPT_RCV.4: Function Recovery, and FRU_FLT.1: Degraded Fault Tolerance, which ensure that the TOE can return to a secure state.

OE.Guide_Docs: Guidance Documentation
Deter installation, configuration and operating errors by providing installation, configuration, operating, and procedural guidance documentation on a timely basis. Guidance Documentation will also assist personnel in the maintenance of the TOE and TOE security functions.

OE.Guide_Docs is assured for the TOE by AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance, ALC_DVS.1: Identification of Security Measures, and by ADV_SPM.1: Informal TOE Security Policy Model, which ensures that guidance is provided to those in network management roles, including security documentation. OE.Guide_Docs is also assured by ADV_FSP.2: Fully Defined External Interfaces, ALC_FLR.3: Systematic Flaw Remediation, AMA_EVD.1: Evidence of Maintenance Process, AVA_MSU.1: Examination of Guidance and AVA_VLA.1: Developer Vulnerability Analysis, which requires guidance documentation to identify all modes of operation and vulnerabilities.

O.Lifecycle: Lifecycle Security
The TOE will be managed and maintained such that its security functions are implemented and preserved throughout its operational lifetime. Upgrades made to the hardware, software or firmware will preserve or enhance current security features without affecting any other TSF.

O.Lifecycle is implemented in the TOE by FPT_AMT.1: Abstract Machine Testing, and FPT_TST.1: TSF Testing, which requires self-tests to ensure correct operation of the TSF. O.Lifecycle is also implemented by FPT_TDC.1: Inter-TSF Basic TSF Data Consistency, which requires the ability to consistently interpret TSF data.

O.Mgmt_Path: Trusted Path for Management Data
Provide integrity and confidentiality of all management data transferred between the TOE and the network management station. Provide a trusted path that is distinct from and cannot be confused with other communications. To aid in providing confidentiality, the TOE must be able to support a cryptographic infrastructure. The cryptographic infrastructure will support services including client registration, key management and segregation of communities of interest.

O.Mgmt_Path is implemented in the TOE by FTP_TRP.1: Trusted Path, FPT_ITI.1: Inter-TSF Detection of Modification, FDP_ITC.2: Import from Outside TSF Control, FDP_UIT.1: Data Exchange Integrity, and FDP_ETC.2: Export of User Data with Security Attributes, which provides integrity and confidentiality of Management data during transmission. O.Mgmt_Path is also implemented by FDP_IFF.1: Simple Security Attributes, which requires a trusted path for management information.

O.Patches: Security Fixes and Patches
The TOE has the latest patches and security fixes installed.

O.Patches is implemented in the TOE by FMT_MOF.1: Management of Security Functions Behavior, which requires Network Management Security Administrators to be responsible for the installation of TOE security fixes and patches. O.Patches is assured by ALC_FLR.3: Systematic Flaw Remediation, which requires that flaw remediation procedures include the distribution of corrections for the flaw.

OE.Personnel: Trustworthy Personnel
Attempt to hire and retain trustworthy and competent personnel. Examples of how these characteristics will be ensured include security lectures, polygraphing, monitoring, misuse detection analysis/auditing, and testing. Personnel shall be initially trained and continuous training shall be provided.

OE.Personnel is assured for the TOE by AGD_ADM.1: Administrator Guidance, and AGD_USR.1: User Guidance, which requires descriptions of the behavior of those in network management roles for the secure operation of the TOE. OE.Personnel is also implemented by FMT_MOF.1: Management of Security Functions Behavior, FMT_MSA.1: Management of Security Attributes and FMT_MSA.3: Static Attribute Initialization, all of which assign trusted responsibilities to Network Management Security Administrators, Network Management Administrators and Network Performance Management Operators.

OE.Physical: Physical Protection
Resources should be physically protected to prevent malicious attacks, unauthorized modification, destruction and theft.

OE.Physical is implemented by FPT_PHP.1: Passive Detection of Physical Attack, which requires that the TOE recognizes a physical attack.

O.Priority_Of_Service: Provide Priority of Service
Assign priorities to all traffic streams, even if all priorities are set for best effort. Control access to resources so that lower-quality/priority classes of service do not unduly interfere with or delay higher-quality/priority classes of service.

O.Priority_Of_Service is implemented in the TOE by FRU_PRS.2: Full Priority of Service, which requires the assignment of priorities, by FRU_FLT.1: Degraded Fault Tolerance, which ensures the preservation of priority of service when a failure occurs and O.Priority_Of_Service is also implemented by FDP_IFF.1: Simple Security Attributes which requires that priority be given to information received from trusted services.

O.Protect_Addresses: Protect Addresses
The TOE will protect the confidentiality and integrity of the transmitting and receiving authorized organizations' internal addresses. Upon receipt, the TOE will correctly interpret both originating and destination authorized addresses.

O.Protect_Addresses is implemented in the TOE by FTP_TRP.1: Trusted path, FTP_ITC.1: Inter-TSF Trusted Channel, FDP_ITC.2: Import from Outside TSF Control, FDP_ETC.2 Export of User Data with Security Attributes, and FPT_ITC.1: Inter-TSF Confidentiality during Transmission, which enforce TOE security functions in order to protect addresses through the prevention of: disclosure, modification, re-ordering of, or loss of data.

O.Protocols: Protocols
Standardized protocols shall be implemented in the TOE to achieve interoperability with switches/routers of other vendors. Protocols shall be implemented in the TOE to provide reliable transport and error detection.

O.Protocols is implemented in the TOE by FDP_ETC.2: Export of User Data with Security Attributes which requires the TOE to ensure integrity, and by FDP_ITC.2: Import of User Data with Security Attributes to ensure integrity and that protocols clearly associate security attributes with data. O.Protocols is also implemented by FDP_UIT.1: Data Exchange Integrity, FPT_FLS.1: Failure with Preservation of Secure State, and FPT_ITI.1: Inter-TSF Detection of Modification to detect errors or modifications during transport of the data

O.Replay_Prevent: Prevent Replay Attacks
The TOE will be capable of rejecting old or duplicate packets in order to protect itself against a replay attack where an unauthorized agent may be masquerading as an authorized agent.

O.Replay_Prevent is implemented in the TOE by FDP_ITC.2: Import from Outside TSF Control, FDP_ETC.2: Export of User Data with Security Attributes, FPT_ITI.1: Inter-TSF Detection of Modification, FDP_UIT.2: Source Data Exchange Recovery, and FPT_RPL.1: Replay Detection, which require the detection of re-played messages and the enforcement of anti-replay.

OE.Synchronization: Network Synchronization
The TOE shall be connected to a reliable time source to allow for the proper synchronization of network resources.

OE.Synchronization is implemented by FMT_MOF.1: Management of Security Functions Behavior and by FPT_STM.1: Reliable Time Stamps, which requires a connection to a reliable time source.

O.Test: Testing of the TOE and TSF
Test plans and procedures will be written and followed to test the TOE and the TSF. Vulnerability testing will be conducted to search for methods of how the TOE Security Policy can be violated. All test methods and results will be documented.

O.Test is implemented by FPT_TST.1: TSF_Testing, FPT_AMT.1: Abstract Machine Testing, which require tests to ensure the correct operation of the TOE and the TSF. O.Test is assured by AMA_SIA.2: Examination of Security Impact Analysis, ATE_COV.2: Analysis of Coverage, ATE_FUN.1: Functional Testing, ATE_IND.2: Independent Testing, AVA_SOF.1: Strength of TOE Security Function Evaluation, and byAVA_VLA.1: Developer Vulnerability Analysis, all of which require testing and analysis of the TOE features and functions or

vulnerability testing.

O.Traf_Audit: Audit Traffic Records with Identity
Record in audit records traffic and performance statistics including, but not limited to, the date, time, size of traffic data sent (cells/packets per second, kbps, mbps, etc.), size of traffic data received (cells/packets per second, kbps, mbps, etc.), node identifiers and organization responsible for the transmission of data. Ensure the integrity of all audit records. The TOE does not have to be responsible for storing these traffic audit records.

O.Traf_Audit is implemented by FAU_GEN.1: Audit Data Generation, FPT_TDC.1: Inter-TSF basic TSF Data Consistency, FAU_SAR.1: Audit Review, and FAU_SEL.1: Selective Audit, which require the generation, easy to interpret format and customizable capabilities of audited events. O.Traf_Audit is also implemented by FAU_GEN.2: User Identity Association, which requires the capture and ability to associate the responsible party with the audited event, by FPT_STM.1: Reliable Time Stamps which requires the capture of the accurate time which can be associated with the audited event, and by FDP_IFF.1: Simple Security Attributes which requires the ability to audit the receipt and acceptance of traffic from untrusted sources.

O.Trust_Backup: Integrity and Confidentiality of System Data Replication
Ensure that all network files and configuration parameters of the TOE are replicated. The file backup will occur on a regular basis. The data will be consistent and properly stored in accordance with the network security policy so that file integrity and confidentiality is ensured. The backup files will be sufficient to re-create the configuration of the TOE in order to restore the TOE to proper operation in the event of a failure or security compromise. The network files may be replicated by automatically being backed-up to a second management station on a regular basis.

O.Trust_Backup is implemented by FDP_UIT.2: Source Data Exchange Recovery, which requires the backup of management data in order to ensure continuous operation of the TOE.

O.Trusted_Recovery: Trusted Recovery
Ensure the recovery to a secure state, without security compromise, after a discontinuity of operations. Ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the network.

O.Trusted_Recovery is implemented in the TOE by FPT_RCV.3: Automated Recovery Without Undue Loss, and FPT_RCV.4: Function Recovery, which require the recovery to a secure state after a discontinuity of operation. FPT_FLS.1: Failure with Preservation of Secure State, also implements this

objective by requiring that a secure state be preserved when a failure occurs in order to be able to recover to a secure state.

O.Unused_Fields: Unused Fields
Ensure that values for all unused fields within the header are properly set. If these fields are not used they will be blocked or reset

O.Unused_Fields is implemented in the TOE by FPT_ITI.1: Inter-TSF Detection of Modification, by requiring that the TSF be able to detect any modifications of TSF data during transmission. Fields within the header can be considered part of TSF data.

O.Validation: Validation of HW/SW/FW
Ensure, through features and procedures, the integrity of all hardware, software and firmware and that all hardware, software and firmware is correctly installed and functioning properly.

O.Validation is implemented in the TOE by FPT_AMT.1: Abstract Machine Testing, and FPT_TST.1: TSF Testing, by requiring tests that will help verify the correct operation and functionality of the TOE and all its components.

6.3 SECURITY FUNCTIONAL REQUIREMENTS GROUNDING IN OBJECTIVES

This section is summarized and provides evidence of comprehensive coverage of each requirement.

Table 6-4 Requirements to Objectives Mapping

Requirements	Objectives
ACM_AUT.1	EAL3 Augmented Supporting Selection
ACM_CAP.3	Supporting Selection of EAL3
ACM_SCP.1	Supporting Selection of EAL3
ADO_DEL.1	Supporting Selection of EAL3
ADO_IGS.1	Supporting Selection of EAL3
ADV_FSP.2	EAL3 Augmented Supporting Selection, OE.Guide_Docs
ADV_HLD.2	Supporting Selection of EAL3
ADV_RCR.1	Supporting Selection of EAL3

Requirements	Objectives
ADV_SPM.1	EAL3 Augmented Supporting Selection, OE.Guide_Docs
AGD_ADM.1	Supporting Selection of EAL3, OE.Guide_Docs, OE.Personnel
AGD_USR.1	Supporting Selection of EAL3, OE.Guide_Docs, OE.Personnel
ALC_DVS.1	Supporting Selection of EAL3, OE_Guide_Docs
ALC_FLR.3	EAL3 Augmented Supporting Selection, OE.Guide_Docs, O.Patches
ALC_TAT.1	EAL3 Augmented Supporting Selection
AMA_AMP.1	EAL3 Augmented Supporting Selection
AMA_EVD.1	EAL3 Augmented Supporting Selection, OE.Guide_Docs
AMA_SIA.2	EAL3 Augmented Supporting Selection, O.Test
ATE_COV.2	Supporting Selection of EAL3, O.Test
ATE_DPT.1	Supporting Selection of EAL3
ATE_FUN.1	Supporting Selection of EAL3, O.Test
ATE_IND.2	Supporting Selection of EAL3, O.Test
AVA_MSU.1	Supporting Selection of EAL3, OE.Guide_Docs
AVA_SOF.1	Supporting Selection of EAL3, O.Test
AVA_VLA.1	Supporting Selection of EAL3, OE.Guide_Docs, O.Test
FAU_GEN.1	OE.Admin_Audit, O.Traf_Audit
FAU_GEN.2	OE.Admin_Audit, O.Traf_Audit

Requirements	Objectives
FAU_SAR.1	OE.Admin_Audit, OE.Attr_Mgt, OE.Audit_Review, O.Traf_Audit
FAU_SEL.1	OE.Admin_Audit, O.Traf_Audit,
FDP_ACC.1	O.Access_Control, O.Ctrl_I&A
FDP_ACF.1	O.Access_Control, O.Ctrl_I&A,

Requirements	Objectives
FDP_ETC.2	O.Mgmt_Path, O.Protect_Addresses, O.Protocols, O.Replay_Prevent
FDP_IFC.1	O.Access_Control, O.Ctrl_I&A
FDP_IFF.1	O.Access_Control, O.Ctrl_I&A, O.Ctrl_Channel, O.Mgmt_Path, O.Priority_Of_Service, O.Traf_Audit
FDP_ITC.2	O.Mgmt_Path, O.Protect_Addresses, O.Protocols, O.Replay_Prevent
FDP_UIT.1	O.Ctrl_Channel, O.Mgmt_Path, O.Protocols
FDP_UIT.2	O.Replay_Prevent, O.Trust_Backup
FIA_UAU.2	O.Access_Control, O.Ctrl_I&A
FIA_UID.2	O.Access_Control, O.Ctrl_I&A
FMT_MOF.1	O.Patches, OE.Personnel, OE.Synchronization

FMT_MSA.1	OE.Admin_Audit, OE.Attr_Mgt, OE.Personnel
FMT_MSA.3	OE.Admin_Audit, OE.Personnel
FMT_MTD.1	OE.Admin_Audit, OE.Attr_Mgt
FMT_SMR.2	OE.Attr_Mgt
FPT_AMT.1	O.Alarm, O.Lifecycle, O.Test, O.Validation
Requirements	**Objectives**
FPT_FLS.1	OE.Environment, O.Fail_Secure, O.Protocols, O.Trusted_Recovery
FPT_ITC.1	O.Ctrl_Channel, O.Protect_Addresses
FPT_ITI.1	O.Cfg_Integrity, O.Ctrl_Channel, O.Detect_Connection, O.Mgmt_Path, O.Protocols, O.Replay_Prevent, O.Unused_Fields
FPT_PHP.1	OE.Physical
FPT_RCV.3	OE.Environment, O.Fail_Secure, O.Trusted_Recovery
FPT_RCV.4	OE.Environment, O.Fail_Secure, O.Trusted_Recovery,
FPT_RPL.1	O.Detect_Connection, O.Replay_Prevent
FPT_STM.1	OE.Admin_Audit, OE.Synchronization, O.Traf_Audit
FPT_TDC.1	OE.Admin_Audit, OE.Audit_Review, O.Lifecycle, O.Traf_Audit

FPT_TST.1	O.Alarm, O.Cfg_Integrity, O.Lifecycle, O.Test, O.Validation
FRU_FLT.1	OE.Environment, O.Fail_Secure, O.Priority_Of_Service
FRU_PRS.2	O.Priority_Of_Service
FTA_TSE.1	O.Access_Control, O.Ctrl_I&A

Requirements	Objectives
FTP_ITC.1	O.Cfg_Confidentiality, O.Cfg_Integrity, O.Ctrl_Channel, OE.Cryptography, O.Protect_Addresses
FTP_TRP.1	O.Cfg_Confidentiality, O.Cfg_Integrity, O.Cfg_Manage, OE.Cryptography, O.Mgmt_Path, O.Protect_Addresses

6.4 DEPENDENCY RATIONALE

This section presents comprehensive coverage of requirements and their dependencies.

Table 6-5 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_ETC.2	FDP_ACC.1
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3
FDP_ITC.2	FDP_ACC.1, FTP_ITC.1, FTP_TRP.1, FPT_TDC.1
FDP_UIT.1	FDP_ACC.1 or FDP_IFC.1, FTP_ITC.1 or FTP_TRP.1, FTP_TRP.1
FDP_UIT.2	FDP_ACC.1, FTP_ITC.1

Requirement	Dependencies
FIA_UAU.2	FIA_UID.1
FIA_UID.2	-
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMR.2	FIA_UID.1
FPT_AMT.1	-
FPT_FLS.1	ADV_SPM.1
FPT_ITC.1	-
FPT_ITI.1	-
FPT_PHP.1	FMT_MOF.1
FPT_RCV.3	FPT_TST.1, AGD_ADM.1, ADV_SPM.1
FPT_RCV.4	ADV_SPM.1
FPT_RPL.1	-
FPT_STM.1	-
FPT_TDC.1	-
FPT_TST.1	FPT_AMT.1
FRU_FLT.1	FPT_FLS.1
FRU_PRS.2	-
FTA_TSE.1	-
FTP_ITC.1	-
FTP_TRP.1	-

Assurance Requirements	
Requirement	**Dependencies**
ACM_AUT.1	ACM_CAP.3
ACM_CAP.3	ACM_SCP.1, ALC_DVS.2
ACM_SCP.1	ACM_CAP.3
ADO_DEL.1	-
ADO_IGS.1	AGD_ADM.1
ADV_FSP.2	ADV_RCR.1
ADV_HLD.2	ADV_FSP.2, ADV_RCR.1
ADV_RCR.1	-
ADV_SPM.1	ADV_FSP.2
AGD_ADM.1	ADV_FSP.2
AGD_USR.1	ADV_FSP.2
ALC_DVS.1	-
ALC_FLR.3	-
ALC_TAT.1	ADV_IMP.1
AMA_AMP.1	ACM_CAP.2, ALC_FLR.1, AMA_CAT.1
AMA_EVD.1	AMA_AMP.1, AMA_SIA.1
AMA_SIA.2	AMA_CAT.1
ATE_COV.2	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1
ATE_FUN.1	-
ATE_IND.3	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1

Requirement	Dependencies
AVA_MSU.1	ADO_IGS.1, ADV_FSP.2, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

6.5 RATIONALE FOR EVALUATION ASSURANCE LEVEL 3 - AUGMENTED

For this Protection Profile an Evaluation Assurance Level of 3 was chosen with a few augmented assurances. EAL3 is an appropriate level as the desire is to have near-term implementation of the specified functional and assurance requirements without the need to retrofit existing product lines. A Level of 3 was decided upon after considering many factors, including documented threats, associated risks, functions implemented in currently available commercial products and the strength of these functions. Work that is being done within working groups of standard making bodies, such as the IETF (www.ietf.org) and the ATM Forum (www.atmforum.com) was also examined.

EAL3 permits developers to obtain maximum assurance from security engineering at the design stage without needing to substantially alter existing development practices. EAL3 provides confidence that the TOE will not be tampered with during development. Evaluated level 3 assurance is gained through the analysis and understanding of the security functions and their behaviors. The analysis is supported by functional and interface specifications, guidance documentation and high-level design details, as well as methodical testing of the TOE and the TOE security functions. Evidence and analysis of testing by the developer as well as independent testing is required at EAL3 for assurance of security functionality without substantial re-engineering. During testing and analysis, secure procedures for all modes of operation will be addressed so that non-secure states will be easy to detect. These more complete testing methods provide an increase in assurance from EAL2.

The chosen EAL3 has been augmented for a higher assurance level since EAL4 is not appropriate for the goal of this protection profile. EAL4 requires more design description and enhanced mechanisms and procedures for increased confidence that the

TOE will not be tampered with during development and delivery. Independent vulnerability analysis demonstrating resistance to penetration attackers is also required. EAL4 is more appropriate when developers and their customers require a moderate to high level of independently assured security and are prepared to incur the additional security-specific engineering costs.

The following are the augmented assurance levels from EAL3:

ACM_AUT.1: Partial CM Automation
ADV_FSP.2: Fully Defined External Interfaces
ADV_SPM.1: Informal TOE Security Policy Model
ALC_FLR.3: Systematic Flaw Remediation
ALC_TAT.1: Well-defined Development Tools
AMA_AMP.1:Assurance Maintenance Plan
AMA_EVD.1: Evidence of Maintenance Process
AMA_SIA.2: Examination of Security Impact Analysis

ACM_AUT.1 was chosen for the use of a configuration management system to ensure the integrity of the TOE through the refinement and modification stages of development. ACM_AUT.1 prevents unauthorized modifications, additions or deletions to the TOE thus providing assurance that the TOE and documentation used for evaluation are the ones prepared for distribution.

ADV_FSP.1 is required for EAL3, however, ADV_FSP.2 is desired for assurance that the TOE security functional requirements are completely represented. A complete presentation of functional interfaces will provide the necessary details to support thorough testing of the TOE and assessment of vulnerabilities.

ADV_SPM.1 is not required for EAL3. It is a dependency of FPT_FLS.1: Failure with Preservation of Secure State, FPT_RCV.3: Automated Recovery without Undue Loss, and FPT_RCV.4: Function Recovery. ADV_SPM.1 is desired for the additional assurance that the security policy model provides through the rationale that the security functions in the functional specification enforce the policies in the TSP.

ALC_FLR, at any component level, is not required for any assurance level. ALC_FLR.3 is included so that flaws are tracked and corrected and that information about security flaws is distributed.

ALC_TAT.1 is not required to satisfy EAL3. It is included for the identification of well-defined development tools including, but not limited to, implemented standards and protocols.

None of the families within the Maintenance of Assurance class are required for any of

the evaluation assurance levels. AMA_AMP.1 is included to assure that the developer discloses current plans for any new releases of the TOE. AMA_AMP.1 will also ensure that any changes made to the TOE will not prevent the TOE from meeting its security target by including the discovery of any new threats or vulnerabilities in the assurance maintenance plan.

AMA_EVD.1 is included in conjunction with AMA_AMP.1 to ensure that the assurance maintenance procedures in the assurance maintenance plan are being followed.

AMA_SIA.2 is included for assurance that even though changes have been made to the TOE, security functions have been maintained. The security impact analysis that this requirement describes will provide this assurance.

6.6 Strength of Function Rationale

The strength of function rating of SOF-medium is appropriate for this protection profile and is based on the potentially high value of information that is required to be protected by the TOE when facing the level of threats as described in Section 3.2 – Threats to Security. A Strength of Function rating of medium is reflective of the attack potential against which the security function is designed to protect given the assumption that attackers have a medium level of expertise, resources, and motivation. This strength of function rating is consistent with the security objectives described in Section 4.0 – Security Objectives and is supported by the Required Security Functionalities listed in Section 2.5.

APPENDIX A - ACRONYMS

AAL – Asynchronous Transfer Mode Adaptation LayerAM – Assurance Maintenance
APS – Automatic Protection Switching
ATM – Asynchronous Transfer ModeBGP – Border Gateway Protocol
CC - Common Criteria
CM – Configuration Management
CMIP – Common Management Interface Protocol
EAL - Evaluation Assurance LevelFW - Firmware
HTTP – Hyper Text Transfer Protocol
HW - Hardware
IETF – Internet Engineering Task Force
IP – Internet Protocol
ISSE – Information Systems Security Engineer
IT - Information Technology
Kbps – Kilobits per second
LDP – Label Distribution Protocol
MD5 – Message Digest 5
Mbps – Megabits Per Second
NEBS – Network Equipment Building Standards
NNI – Network to Network Interface
NSA – National Security Agency
OSPF – Open Shortest Path First
PNNI – Private Network to Network Interface
PP - Protection Profile
PSTN – Public Switched Telephone Network
QoS – Quality of Service
RFC – Request For Comment (Internet Engineering Task Force)
Rlogin – Remote login
RMON – Remote Monitoring
Rsh – Remote shell protocol
RSVP – Resource Reservation Protocol
SF - Security Function
SFP - Security Function Policy
SOF - Strength of Function
SNMP – Simple Network Management Protocol
SNMP3 – Simple Network Management Protocol version 3
ST - Security TargetSW – Software
TOE - Target of Evaluation
TSC – TOE Security Function Scope of Control
TSE – TOE Security Environment
TSF – Target Of Evaluation Security Functions
TSFI – TOE Security Function Interface

TSP – Target Of Evaluation Security Policy
UNI – User to Network Interface

APPENDIX B - INDEX OF TERMS

Assignment – The specification of an identified parameter in a component

ATM Adaptation Layer (AAL) – The process/programming by which information in some native mode is adapted to the ATM cell structure in the form of 48-byte ATM payload segments. The AAL allows for the adaptation of the ATM layer to particular services. AALs differ on the basis of the source-destination timing used. AAL1 is for constant bit-rate traffic, AAL2 for connection-oriented, time-dependent variable bit-rate traffic, AAL 3 / 4 for both connection-oriented and connection-less variable bit-rate traffic and AAL5 for connection-oriented, variable bit-rate traffic.

Augmentation – The addition of one or more assurance requirements from Part 3 to an EAL or assurance package.

Automatic Protection Switching (APS) - The ability to recover from failures. A switching mechanism that routes traffic from failed lines to working lines to protect them in the event of a line card failure or cable/fiber cut.

BGP – border gateway protocol is an inter-domain routing protocol for exchanging network reachability information with other BGP systems.

CMIP – Common Management Interface Protocol, an ITU-TSS standard for the message formats and procedures used to exchange management information in order to operate, administer maintain and provision a network.

Common Criteria – The name used historically for this standard in lieu of its official ISO name of "Evaluation Criteria for Information Technology Security Evaluation."

Communications – A transfer of information

Component – The smallest selectable set of elements that may be included in a PP, a ST, or a package

Control Signal – Information flow control signals used to carry status messages, or synchronize data streams.

Cyclic Redundancy Check (CRC) - ATM header CRC field is used to verify the integrity of the ATM header fields.

Dependency – A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet

their objectives.

Evaluation Assurance Level (EAL) – A package consisting of assurance components from Part 3 that represents a point on the Common Criteria predefined assurance scale.

Evaluation Authority – A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Frame Check Sequence (FCS) – A field used for error checking. Any mathematical formula that derives a numeric value based on the bit pattern of a transmitted block of information and uses that value at the receiving end to determine the existence of any transmission errors.

Iteration – The use of a component more than once with varying operations

MD5 – A message digest algorithm, as defined in RFC 1321, that is intended for digital signature applications where a large message has to be 'compressed' in a secure manner before being encrypted with the private key. A message of arbitrary length is taken as input and a 128-bit message digest is produced as output.

Network Address – Addresses referring to a logical, rather than a physical, network device. Identifies a node attached to a network.

Object – An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organizational Security Policies – One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSPF – Open Shortest Path First, a link state, hierarchical routing algorithm that calculates the best path across a router network based on various "costs." Factors such as hop count, security requirements, or bandwidth may be defined as costs. As the network topology changes, OSPF stations immediately exchange link state update messages signaling network changes. At predetermined intervals, OSPF stations exchange full topology information.

PNNI – private network to network interface, ATM Forum specification for distributing topology information between switches and clusters of switches that is used to compute paths through the network. The specification is based on well-known link-state routing techniques and includes a mechanism for automatic configuration in networks in which the address structure reflects the topology.

Protection Profile (PP) – An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Q.2931 – ITU-T specification for establishing, maintaining, and clearing network connections. Provides ATM switch virtual connection specifications and standards.

QoS – quality of service is an indicator of the performance of a transmission system on the Internet and ATM networks that reflects its transmission quality and service availability. QoS is measured in transmission rate, error rates, latency, and other characteristics, and can to some extent be guaranteed to a customer in advance. QoS levels include UBR, VBR, VBR+, CBR, and ABR.

Refinement – The addition of details to a component

RSVP – resource reservation protocol supports the reservation of resources across an IP network. RSVP can be used to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive.

Role - A predefined set of rules establishing the allowed interactions between a client and the TOE.

Router – Routers provide logical paths at OSI layer 3 over dedicated or switched lines. Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

RMON – Remote Monitoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.

rsh - remote shell protocol, protocol that allows a client to execute commands on a remote system without having to log in to the system. For example, rsh can be used to remotely examine the status of a number of access servers without connecting to each communication server, executing the command, and then disconnecting from the communication server.

Security Attribute – Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Function (SF) – A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP) – The security policy enforced by a SF.

Security Objective – A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.

Security Target (ST) – a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection – The specification of one or more items from a list in a component

Signalling - Process of sending a transmission signal over a physical medium for purposes of communication. An ATM-connected device that wants to establish a connection with another such device generates signalling information. The signaling packet contains the ATM network service access point address of the desired ATM endpoint, as well as any QoS parameters required for the connection. If the endpoint can support the desired QoS, it responds with an accept message, and the connection is opened.

SNMP – Simple Network Management Protocol, provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security. SNMP defines the communication protocol used between the network management station and an agent, and the structure of management information (MIB) in the agent. SNMP is described in various RFC's including 1157, 2261, 2262, 2263, 2273 etc.

Strength of Function (SOF) – A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

Subject – An entity within the TSC that causes operations to be performed.

Switch – Switches provide logical paths at OSI layer 2. Network device that filters, forwards, and floods frames based on the destination address of each frame. Connections are established as necessary and terminated when there is no longer a session to support. Switches forward frames from one network to another based on data link layer information.

Target of Evaluation (TOE) – A product or system and its associated guidance documentation that is the subject of an evaluation.

Telnet – Network Virtual Terminal Protocol - Used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in many RFCs including 854, 855 etc.

TOE Resource – Anything useable or consumable in the TOE.

TOE Security Functions (TSF) – A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Data – Data created by and for the TOE, that might affect the operation of the TOE.

TSF Scope of Control (TSC) – The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

UNI – User-Network Interface, ATM Forum specifications (UNI 3.0, 3.1, 4.0) that define the interoperability standard for the interface between ATM-based products (a router or a switch) located in a private network and the ATM switches located within the public carrier networks.